Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

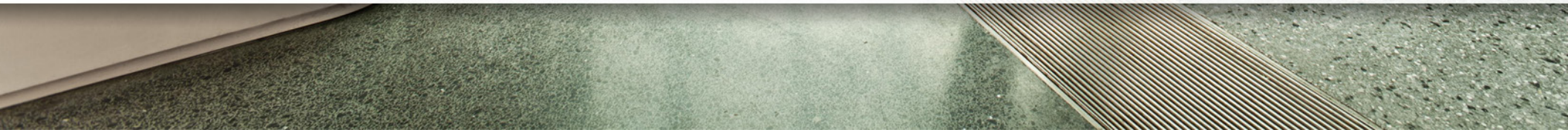
BORDERLESS NETWORKS

DEPLOYMENT GUIDE

Wireless LAN Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series



Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

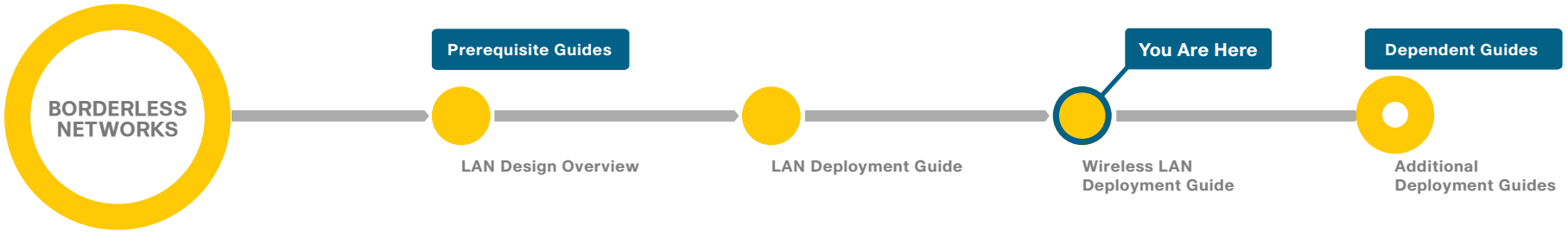
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



Introduction

Business Overview

You can improve the effectiveness and efficiency of employees by allowing them to stay connected, regardless of their location. As an integrated part of the wired networking port design that provides connectivity when users are at their desks or other prewired locations, wireless allows connectivity in transit to meetings and turns cafeterias or other meeting places into ad-hoc conference rooms. Wireless networks enable users to stay connected and the flow of information moving, regardless of any physical building limitations.

Technology Overview

This deployment uses a wireless mobility network in order to provide ubiquitous data and voice connectivity for employees, and wireless guest access for visitors to connect to the Internet.

Regardless of their location within the organization, at large campuses or remote sites, users can connect to voice and data services via the same methods, creating a seamless business environment for the organization.

Benefits

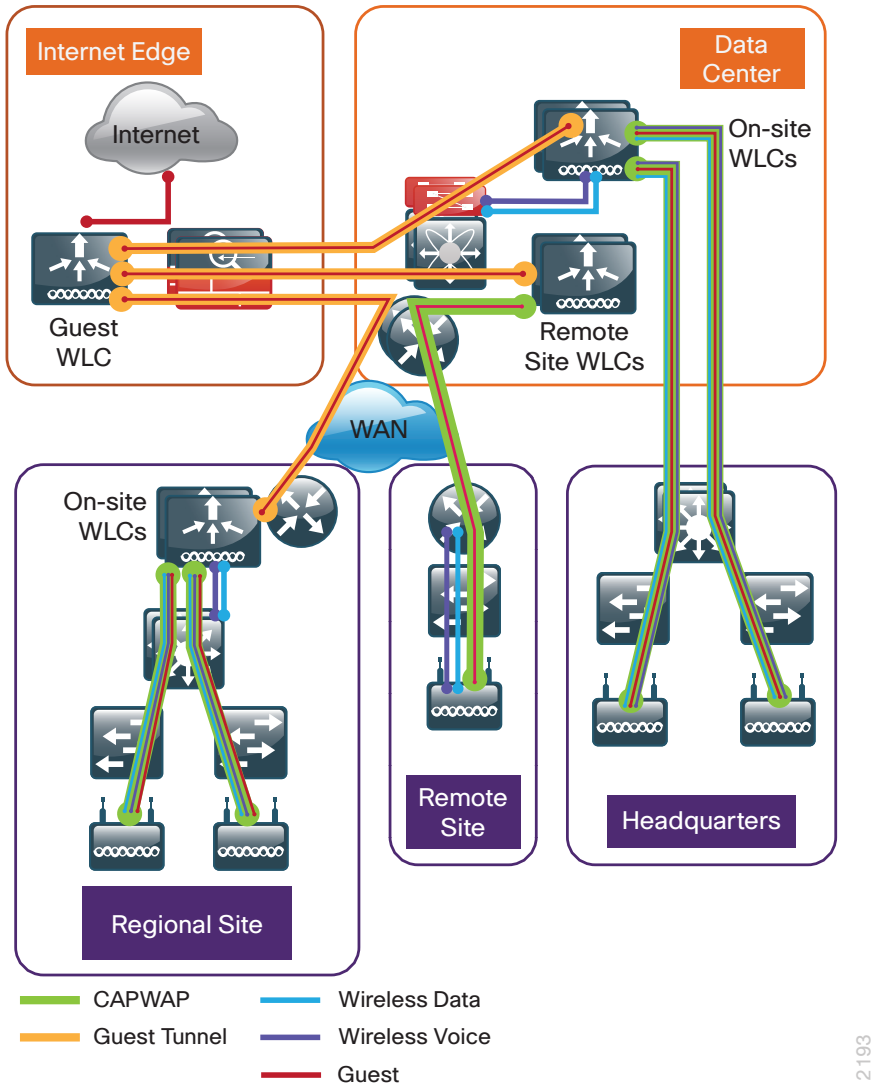
- Location-independent network access—Employee productivity improves.
- Additional network flexibility—Hard-to-wire locations can be reached without costly construction.
- Easy to manage and operate—Organizations have centralized control of a distributed wireless environment.
- Plug-and-play deployment—Network is preconfigured to recognize new access points connected to any access port.

This Cisco® Smart Business Architecture (SBA) deployment uses a controller-based wireless design. Centralizing configuration and control on the Cisco wireless LAN controller (WLC) allows the wireless LAN (WLAN) to operate as an intelligent information network and support advanced services. This centralized deployment simplifies operational management by collapsing large numbers of managed endpoints and autonomous access points into a single managed system.

The following are some of the benefits of a centralized wireless deployment:

- Lower operational expenses—A controller-based, centralized architecture enables zero-touch configurations for lightweight access points. Similarly, it enables easy design of channel and power settings and real-time management, including identifying any RF holes to optimize the RF environment. The architecture offers seamless mobility across the various access points within the mobility group. A controller-based architecture gives the network administrator a holistic view of the network and the ability to make decisions about scale, security, and overall operations.
- Easier way to scale with optimal design—As the wireless deployment scales for pervasive coverage and to address the ever-increasing density of clients, operational complexity starts growing exponentially. In such a scenario, having the right architecture enables the network to scale well. Cisco wireless networks support two deployment models, local mode for campus environments and Cisco FlexConnect™ for lean remote sites.

Figure 1 - Wireless overview



Deployment Components

The Cisco SBA WLAN deployment is built around two main components: Cisco wireless LAN controllers and Cisco lightweight access points.

Cisco Wireless LAN Controllers

Cisco wireless LAN controllers are responsible for systemwide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco lightweight access points to support business-critical wireless applications. From voice and data services to location tracking, Cisco wireless LAN controllers provide the control, scalability, security, and reliability that network managers need to build secure, scalable wireless networks—from large campus environments to remote sites.

Although a standalone controller can support lightweight access points across multiple floors and buildings simultaneously, you should deploy controllers in pairs for resiliency. There are many different ways to configure controller resiliency; the simplest is to use a primary/secondary model where all the access points at the site prefer to join the primary controller and only join the secondary controller during a failure event. However, even when configured as a pair, wireless LAN controllers do not share configuration information. Each wireless LAN controller must be configured separately.

The following controllers are included in this release of Cisco SBA.

- **Cisco 2500 Series Wireless LAN Controller**—The 2504 controller supports up to 50 lightweight access points and 500 clients. Cisco 2500 Series Wireless LAN Controllers are ideal for small, single-site WLAN deployments.
- **Cisco 5500 Series Wireless LAN Controller**—The 5508 controller supports up to 500 lightweight access points and 7000 clients, making it ideal for large site and multi-site WLAN deployments.
- **Cisco Flex® 7500 Series Cloud Controller**—The 7510 controller supports up to 3000 remote site access points and 30,000 clients. This controller is designed to meet the scaling requirements to deploy the Cisco FlexConnect solution in remote site networks.

Because software license flexibility allows you to add additional access points as business requirements change, you can choose the controller that will support your needs long-term, but only pay for what you need, when you need it.

Cisco Lightweight Access Points

In a Cisco Unified Wireless Network architecture, access points are lightweight. This means they cannot act independently of a wireless LAN controller (WLC). The lightweight access points (LAPs) have to first discover the WLCs and register with them before the LAPs service wireless clients. There are two primary ways that the access point can discover a WLC.

- Domain Name System (DNS)—When a single WLC pair is deployed in an organization, the simplest way to enable APs to discover a WLC is by creating a DNS entry for cisco-capwap-controller that resolves to the management IP addresses of WLCs.
- Dynamic Host Configuration Protocol (DHCP)—When multiple WLC pairs are deployed in an organization, use DHCP Option 43 to map access points to their WLCs. Using Option 43 allows remote sites and each campus to define a unique mapping.

As the access point communicates with the WLC resources, it will download its configuration and synchronize its software/firmware image, if required.

The Cisco Lightweight Access Points work in conjunction with a Cisco Wireless LAN Controller to connect wireless devices to the LAN while supporting simultaneous data forwarding and air monitoring functions. The Cisco SBA wireless design is based on Cisco 802.11n wireless access points, which offer robust wireless coverage with up to nine times the throughput of 802.11a/b/g networks.

The following access points are included in this release of Cisco SBA:

- The Cisco Aironet 1040 Series Access Point is an enterprise-class, entry-level access point designed to address the wireless connectivity needs of small- and medium-sized organizations. With 2x2 multiple-input multiple-output (MIMO) technology, this access point provides at least six times the throughput of existing 802.11a/g networks.

Wireless networks are more than just a convenience, they are mission-critical to the business. However, wireless operates in a shared spectrum with a variety of applications and devices competing for bandwidth in enterprise environments. More than ever, IT managers need to have visibility into their wireless spectrum to manage RF interference and prevent unexpected downtime. Cisco CleanAir provides performance protection for 802.11n networks. This silicon-level intelligence creates a self-healing, self-optimizing wireless network that mitigates the impact of wireless interference. This release of SBA includes two CleanAir APs.

- The Cisco 2600 Series Access Points with CleanAir technology create a self-healing, self-optimizing wireless network. By intelligently avoiding interference, they provide the high-performance 802.11n connectivity for mission-critical mobility and performance protection for reliable application delivery.
- The Cisco 3600 Series Access Point with CleanAir technology delivers more coverage for tablets, smart phones, and high-performance laptops. This next-generation access point is a 4x4 MIMO, three-spatial-stream access point resulting in up to three times more availability of 450 Mbps rates, and optimizing the performance of more mobile devices.

For more information on Cisco CleanAir, please read the *Cisco SBA—Borderless Networks Wireless LAN CleanAir Deployment Guide*.

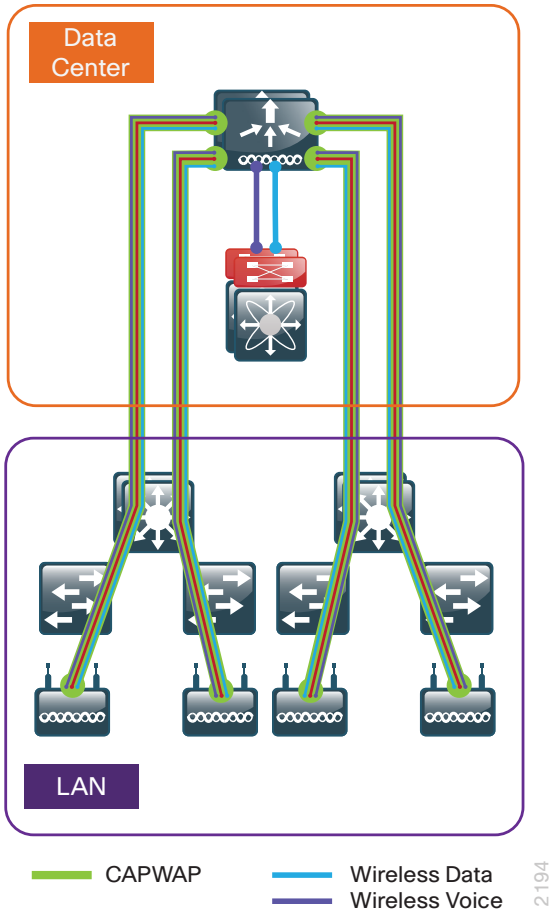
Deployment Models

Cisco Unified Wireless networks support two major deployment models: Local mode and Cisco FlexConnect.

Local-Mode Deployment

In a local-mode deployment, the wireless LAN controller and access points are co-located at the same site. The wireless LAN controller is connected to a LAN distribution layer at the site, and traffic between wireless LAN clients and the LAN is tunneled in Control and Provisioning of Wireless Access

Points (CAPWAP) protocol between the controller and the access point.



A local-mode architecture uses the controller as a single point for managing Layer 2 security and wireless network policies. It also enables services to be applied to wired and wireless traffic in a consistent and coordinated fashion.

In addition to providing the traditional benefits of a Cisco Unified Wireless Network approach, the local-mode deployments have the following custom demands:

- **Seamless mobility**—In a campus environment, it is crucial that users remain connected to their session even while walking between various floors or adjacent buildings with changing subnets. The local controller–based Cisco Unified Wireless Network enables fast roaming across the campus.
- **Ability to support rich media**—As wireless has become the primary mode of network access in many campus environments, voice and video applications have grown in significance. Local-mode deployments enhance robustness of voice with Call Admission Control (CAC) and multicast with Cisco VideoStream technology.
- **Centralized policy**—The consolidation of data at a single place in the network enables intelligent inspection through the use of firewalls, as well as application inspection, network access control, and policy enforcement. In addition, network policy servers enable correct classification of traffic from various device types and from different users and applications.

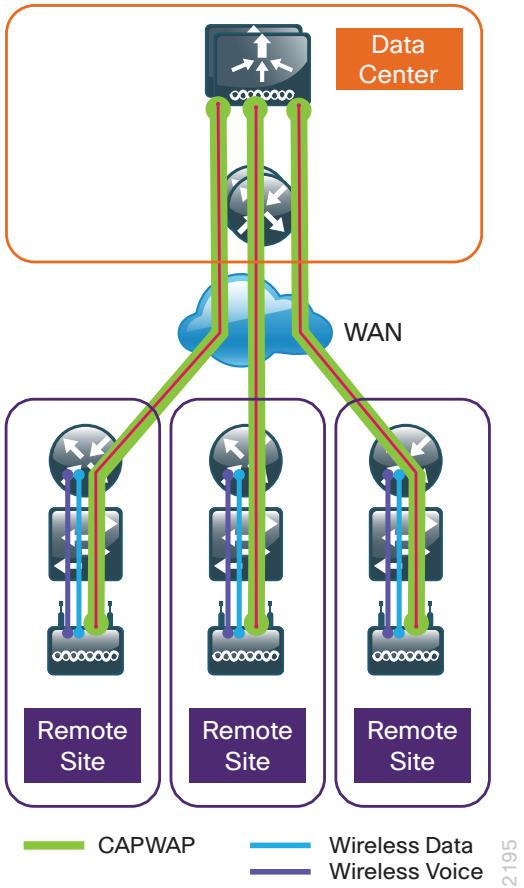
If any of the following are true at a site, you should deploying a controller locally at the site:

- The site has a LAN distribution layer.
- The site has more than 50 access points.
- The site has a WAN latency greater than 100 ms round-trip to a proposed shared controller.

In a deployment with these characteristics, use either a Cisco 2500 or 5500 Series Wireless LAN Controller. For resiliency, the design uses two wireless LAN controllers for the campus, although you can add more wireless LAN controllers to provide additional capacity and resiliency to this design.

Cisco FlexConnect Deployment

Cisco FlexConnect is a wireless solution for remote-site deployments. It enables organizations to configure and control access points in a remote site from the headquarters through the WAN without deploying a controller in each remote site.



If all of the following are true at a site, deploy Cisco FlexConnect at the site:

- The site LAN is a single access layer switch or switch stack.
- The site has fewer than 50 access points.
- The site had a WAN latency less than 100 ms round-trip to the shared controller.

The Cisco FlexConnect access point can switch client data traffic out its local wired interface and can use 802.1Q trunking to segment multiple WLANs. The trunk native VLAN is used for all CAPWAP communication between the access point and the controller.

Cisco FlexConnect can also tunnel traffic back to the controller, which is specifically used for wireless guest access.

You can deploy Cisco FlexConnect using a shared controller pair or a dedicated controller pair.

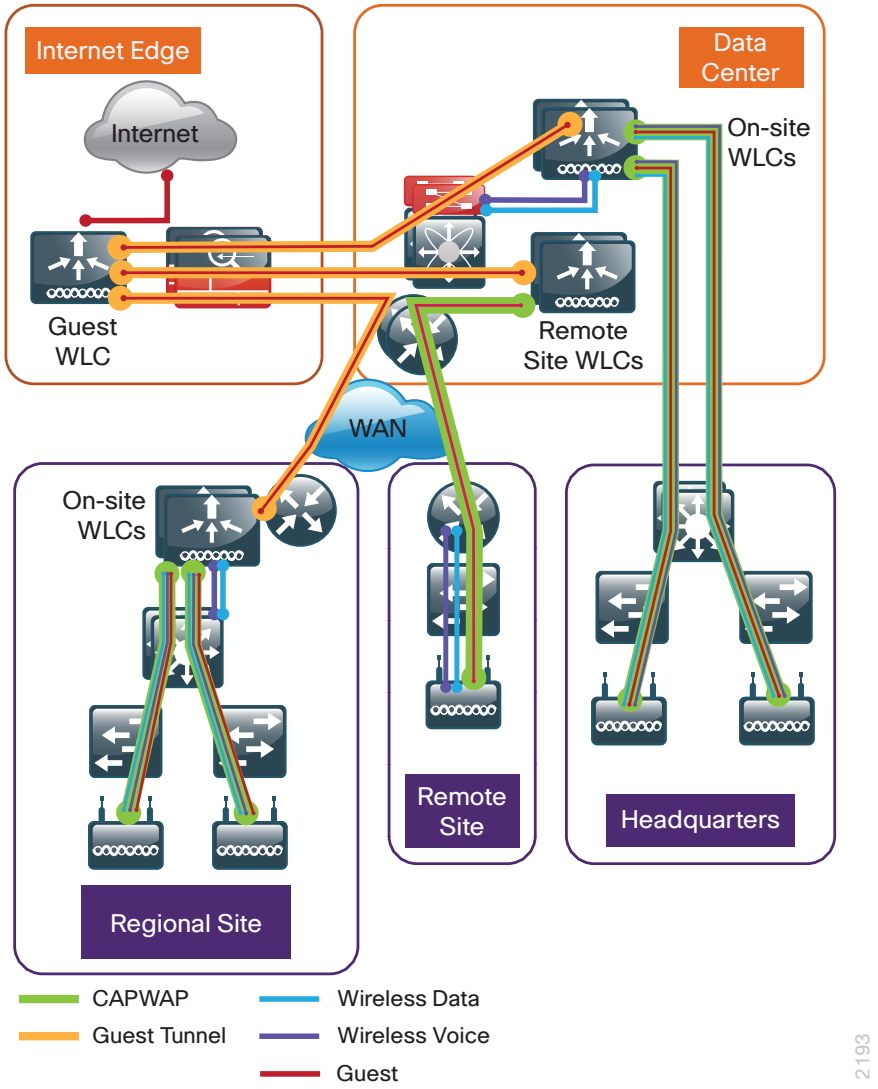
If you have an existing local-mode controller pair at the same site as your WAN aggregation, and the controller pair has enough additional capacity to support the Cisco FlexConnect access points, you can use a shared deployment. In a shared deployment, the controller pair supports both local-mode and Cisco FlexConnect access points concurrently.

If you don't meet these requirements, you can deploy a dedicated controller pair using either the Cisco 5500 Series Wireless LAN Controller or a Cisco Flex 7500 Series Cloud Controller. The controller should be connected to the server room or data center. For resiliency, the design uses two controllers for the remote sites, although you can add more controllers to provide additional capacity and resiliency to this design.

Guest Wireless

Using the organization's existing WLAN for guest access provides a convenient, cost-effective way to offer Internet access for visitors and contractors. The wireless guest network provides the following functionality:

- Provides Internet access to guests through an open wireless Secure Set Identifier (SSID), with web access control.
- Supports the creation of temporary authentication credentials for each guest by an authorized internal user.
- Keeps traffic on the guest network separate from the internal network to prevent a guest from accessing internal network resources.
- Supports both local mode and Cisco FlexConnect deployment models.



You can deploy a wireless guest network using a shared controller pair or a dedicated controller in the Internet DMZ.

If you have one controller pair for the entire organization, and that controller pair is connected to the same distribution switch as the Internet edge firewall, you can use a shared deployment. In a shared deployment, a VLAN is created on the distribution switch to logically connect guest traffic from the WLCs to the DMZ. The VLAN will not have an associated Layer 3 interface or Switch Virtual Interface (SVI), and the wireless clients on the guest network will point to the Internet edge firewall as their default gateway.

If you don't meet the requirements for a shared deployment you can deploy a dedicated guest controller using the Cisco 5500 Series Wireless LAN Controller. The controller is directly connected the Internet edge DMZ, and guest traffic from every other controller in the organization is tunneled to this controller.

In both the shared and dedicated guest deployment model, the Internet edge firewall restricts access from the guest network. The guest network is only able to reach the Internet and the internal DHCP and DNS servers.

Deployment Details

This deployment guide uses certain standard design parameters and references various network infrastructure services that are not located within the wireless LAN (WLAN). These parameters are listed in the following table. Enter the values that are specific to your organization in the "Site-specific values" column.

Table 1 - Universal design parameters

Network service	Cisco SBA values	Site specific values
Domain name	cisco.local	
Active Directory, DNS server, DHCP server	10.4.48.10	
Network Time Protocol (NTP) server	10.4.48.17	
SNMP read-only community	cisco	
SNMP read/write community	cisco123	

Process

Configuring the RADIUS Server: Cisco ACS

1. Create the wireless device type group
2. Create the TACACS+ shell profile
3. Modify the device admin access policy
4. Create the network access policy
5. Modify the network access policy
6. Create the network device
7. Enable the default network device

Cisco® Secure Access Control System (ACS) is the centralized identity and access policy solution that ties together an organization's network access policy and identity strategy. Cisco Secure ACS operates as a centralized authentication, authorization, and accounting (AAA) server that combines user authentication, user and administrator access control, and policy control in a single solution.

Cisco Secure ACS 5.3 uses a rule-based policy model, which allows for security policies that grant access privileges based on many different attributes and conditions in addition to a user's identity.

This guide assumes that you have already configured Cisco Secure Access Control System (ACS). Only the procedures required to support the integration of wireless into the deployment are included. Full details on Cisco ACS configuration are included in the *Cisco SBA—Borderless Networks Device Management using ACS Deployment Guide*.

For information about configuring the RADIUS server on Windows Server 2008, skip to the next process.

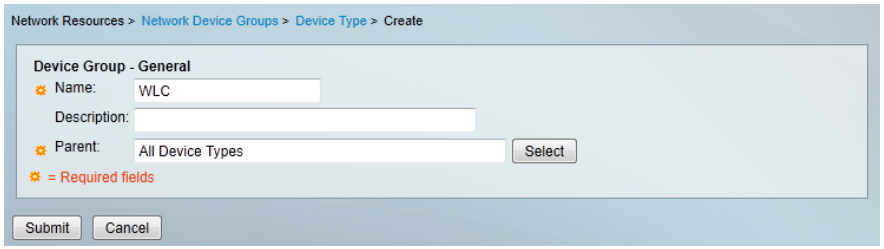
Procedure 1 Create the wireless device type group

Step 1: Navigate to the Cisco ACS Administration Page. (Example: https://acs.cisco.local)

Step 2: In **Network Resources** > **Network Device Groups** > **Device Type**, click **Create**.

Step 3: In the **Name** box, enter a name for the group. (Example: WLC)

Step 4: In the **Parent** box, select **All Device Types,** and then click **Submit**.



Procedure 2 Create the TACACS+ shell profile

You must create a shell profile for the WLCs that contains a custom attribute that assigns the user full administrative rights when the user logs in to the WLC.

Step 1: In **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, click **Create**.

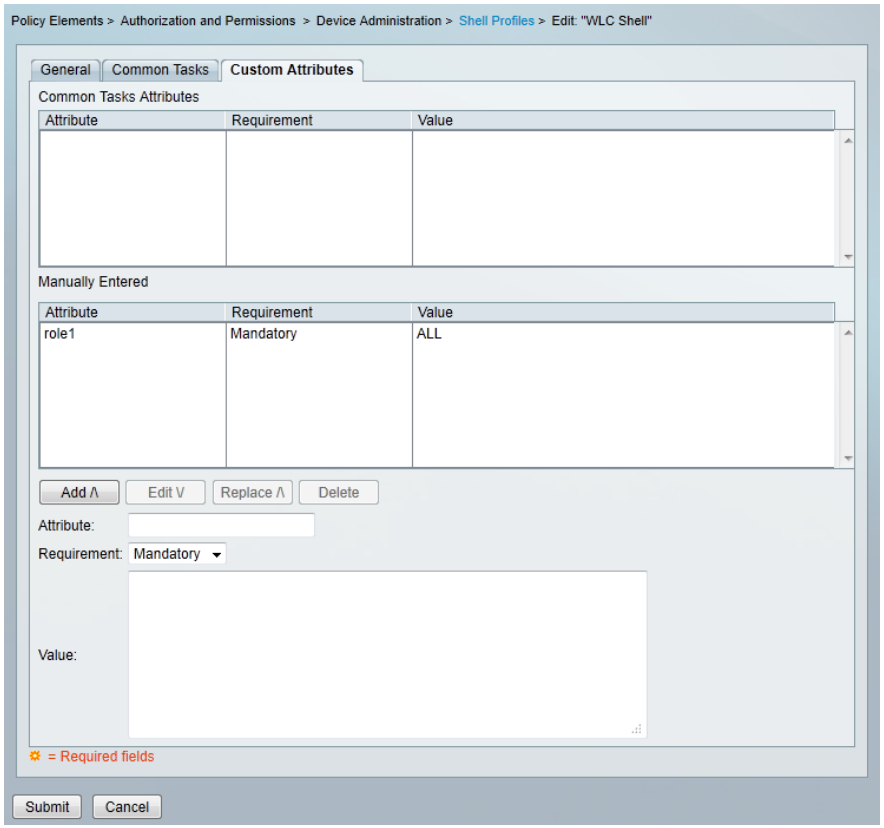
Step 2: Under the General tab, In the **Name** box, enter a name for the wireless shell profile. (Example: WLC Shell)

Step 3: On the Custom Attributes tab, in the **Attribute** box, enter **role1**.

Step 4: In the Requirement list, choose **Mandatory**.

Step 5: In the **Value** box, enter **ALL**, and then click **Add**.

Step 6: Click **Submit**.



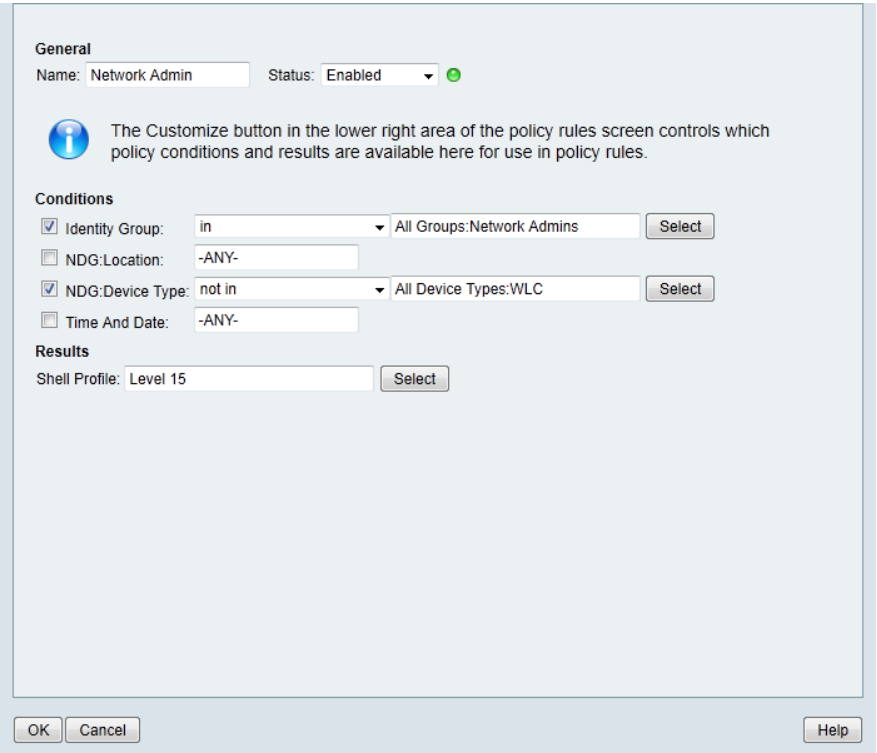
Procedure 3 Modify the device admin access policy

First, you must exclude WLCs from the existing authorization rule.

Step 1: In **Access Policies > Default Device Admin >Authorization,** click the **Network Admin** rule.

Step 2: Under Conditions, select **NDG:Device Type**, and from the filter list, choose **not in**.

Step 3: In the box to the right of the filter list, select **All Device Types:WLC**, and then click **OK**.



Next, create a WLC authorization rule.

Step 4: In **Access Policies** > **Default Device Admin** >**Authorization**, click **Create**.

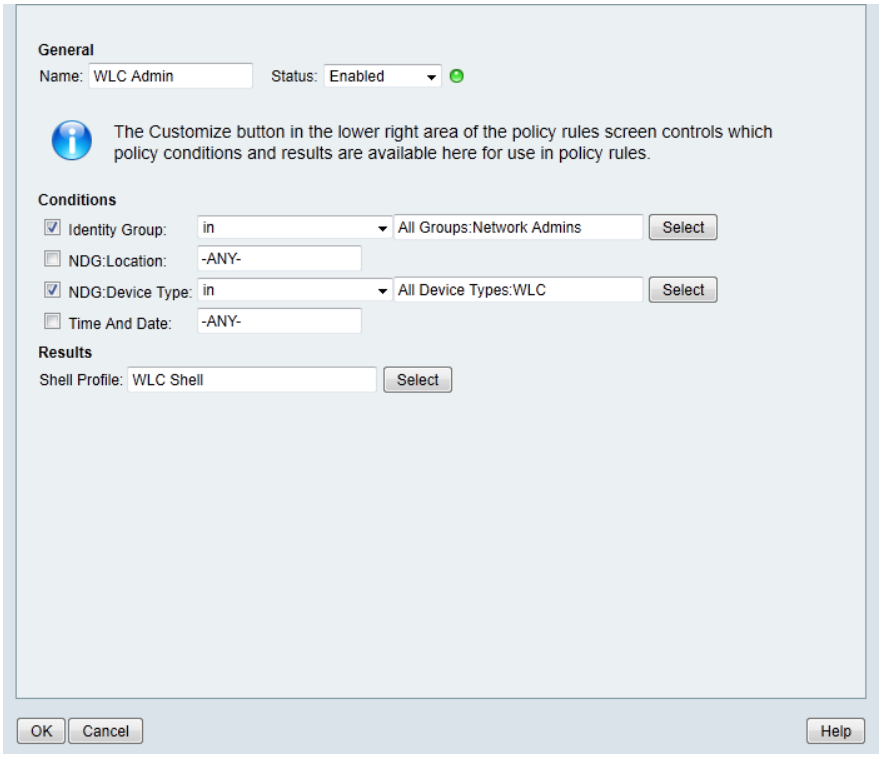
Step 5: In the **Name** box, enter a name for the WLC authorization rule. (Example: WLC Admin)

Step 6: Under Conditions, select **Identity Group** condition, and in the box, select **Network Admins**.

Step 7: Select **NDG:Device Type** , and in the box, select **All Device Types:WLC.**

Step 8: In the **Shell Profile** box, select **WLC Shell**, and then click **OK**.

Step 9: Click **Save Changes**.

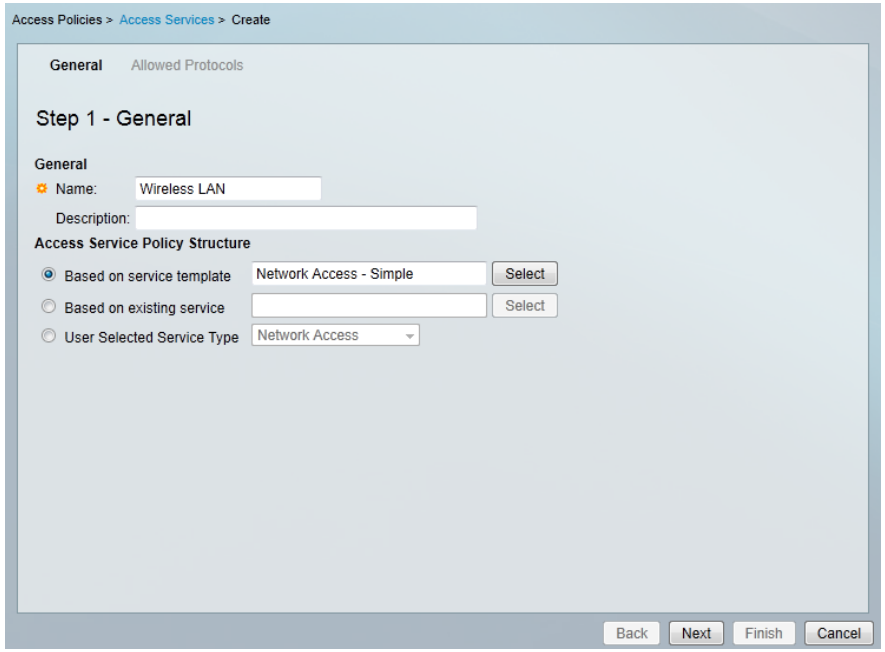


Procedure 4 Create the network access policy

Step 1: In **Access Policies** > **Access Services**, click **Create**.

Step 2: In the Name box, enter a name for the policy. (Example: Wireless LAN)

Step 3: To the right of Based on Service Template, select **Network Access - Simple**, and then click **Next**.



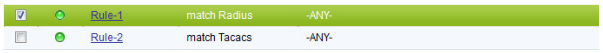
Step 4: On the Allowed Protocols pane, click **Finish**.

Step 5: On the message "Access Service created successfully. Would you like to modify the Service Selection policy to activate this service?", click **Yes**.

Step 6: On the Service Selection Policy pane, click **Customize.**

Step 7: Using the arrow buttons, move Compound Condition from the Available list to the Selected list, and then click **OK**.

Step 8: On the Service Selection Rules pane, select the default Radius rule.



Step 9: Create a new rule for wireless client authentication, click **Create > Create Above**.

Step 10: In the Name box, enter a name for the Rule. (Example: Rule-3)

Step 11: Under conditions, select **Compound Condition**.

Step 12: In the Dictionary list, choose **RADIUS-IETF**.

Step 13: In the Attribute box, select **Service-Type**.

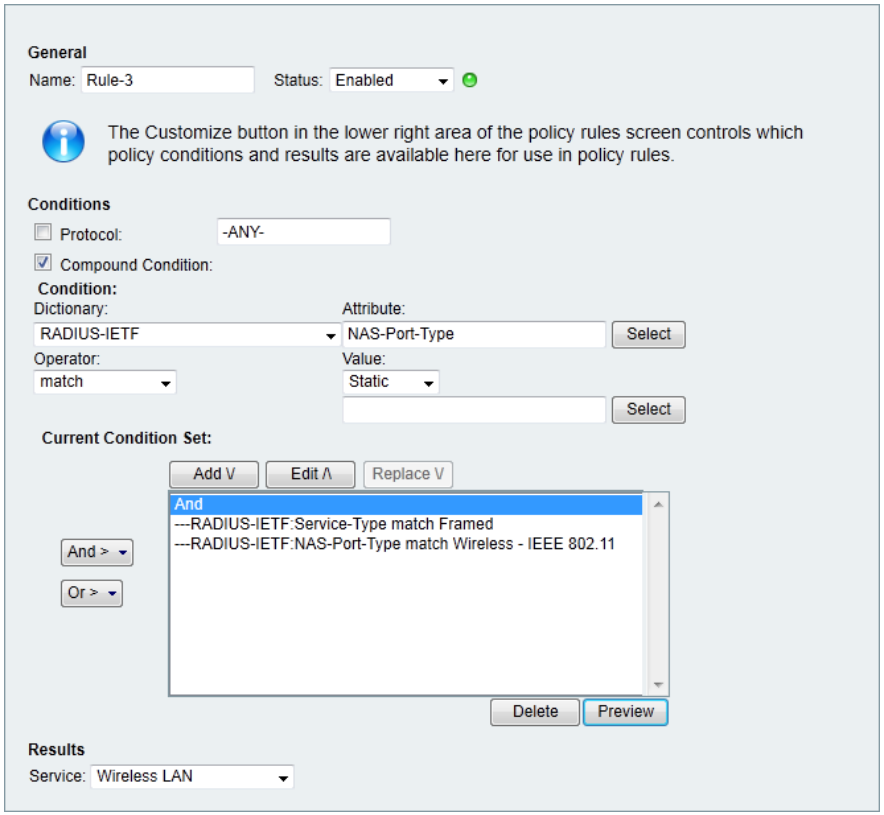
Step 14: In the Value box, select **Frame**, and then click **Add V**.

Step 15: Under current condition set, click **And > Insert**

Step 16: In the Attribute box, select **NAS-Port-Type**.

Step 17: In the Value box, select **Wireless - IEEE 802.11**, and then click **Add**.

Step 18: Under results, in the service list, choose **Wireless LAN**, and then click **OK**.



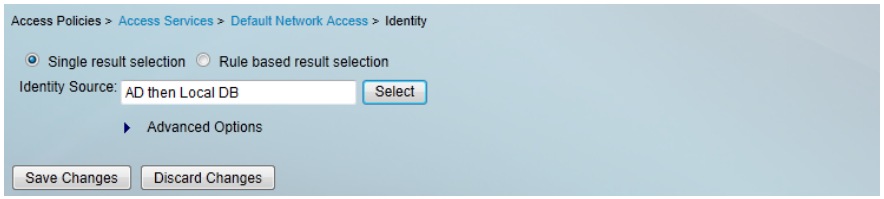
Step 19: On the Service Selection Rules pane, click **Save Changes**.

Procedure 5 Modify the network access policy

Step 1: First you must, create an authorization rule to allow the WLCs to authenticate clients using RADIUS.

Step 2: Navigate to **Access Policies > Wireless LAN > Identity**.

Step 3: In the **Identity Source** box select **AD then Local DB**, and then click **Save Changes**.



Step 4: Navigate to **Access Policies > Wireless LAN > Authorization.**

Step 5: On the Network Access Authorization Policy pane, click **Customize.**

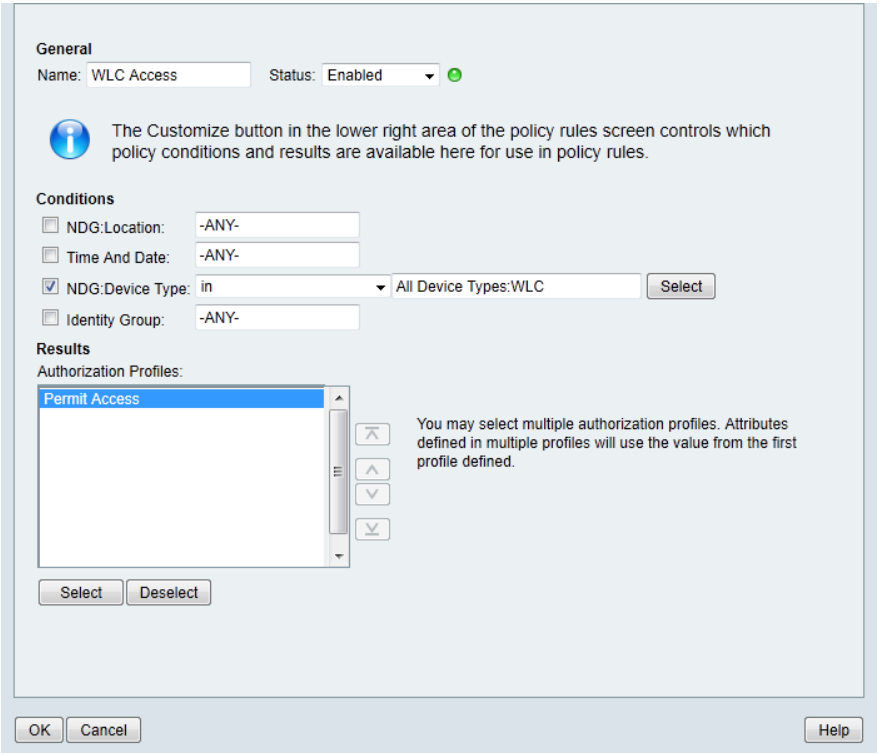
Step 6: Using the arrow buttons, move **NDG:Device Type** from the Available list to the Selected list, and then click **OK**.

Step 7: In **Access Policies > Wireless LAN > Authorization**, click **Create**.

Step 8: In the **Name** box, enter a name for the rule. (Example: WLC Access)

Step 9: Under Conditions, select **NDG:Device Type**, and in the box, select **All DeviceTypes:WLC**.

Step 10: In the **Authorization Profiles** box, select **Permit Access**, and then click **OK**.



Step 11: Click **Save Changes**.

Procedure 6 Create the network device

The TACACS+ shell profile that is required when managing the controllers with AAA must be applied to the controllers. This requires that for each controller in the organization; create a network device entry in Cisco ACS.

Step 1: In **Network Resources > Network Devices and AAA Clients**, click **Create**.

Step 2: In the **Name** box, enter the device host name. (Example: WLC-1)

Step 3: In the **Device Type** box, select **All Device Types:WLC**.

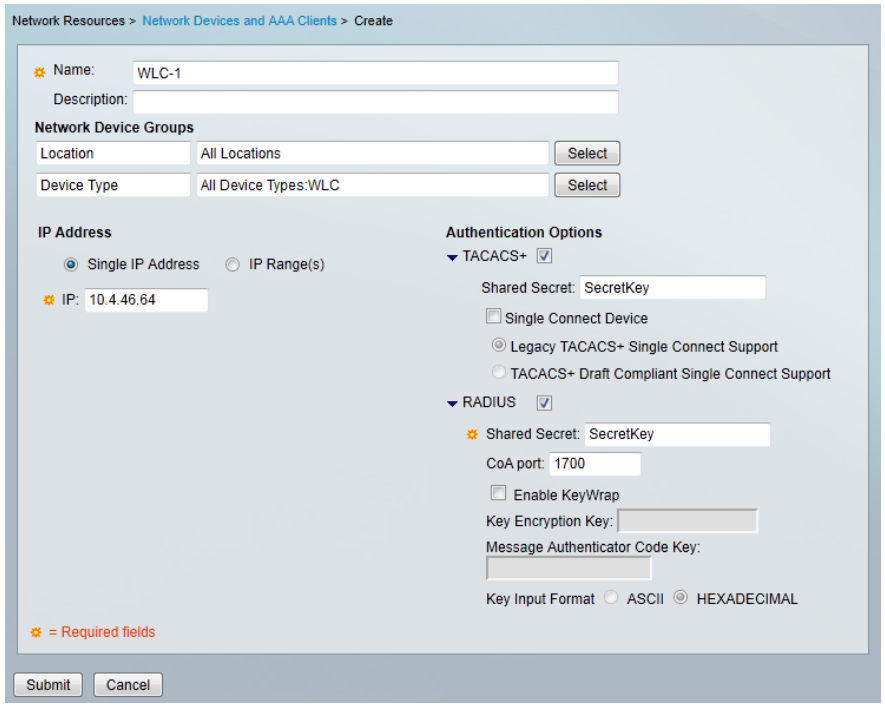
Step 4: In the **IP** box, enter the WLCs management interface IP address. (Example: 10.4.46.64)

Step 5: Select **TACACS+**.

Step 6: Enter the TACACS+ shared secret key. (Example: SecretKey)

Step 7: Select **RADIUS**.

Step 8: Enter the RADIUS shared secret key, and then click **Submit**. (Example SecretKey)



Procedure 7 Enable the default network device

Access points, when they are configured for FlexConnect operation, can authenticate wireless clients directly to ACS, when the controller is unavailable. Enable the default network device for RADIUS to allow the access points to communicate with ACS without having a network device entry.

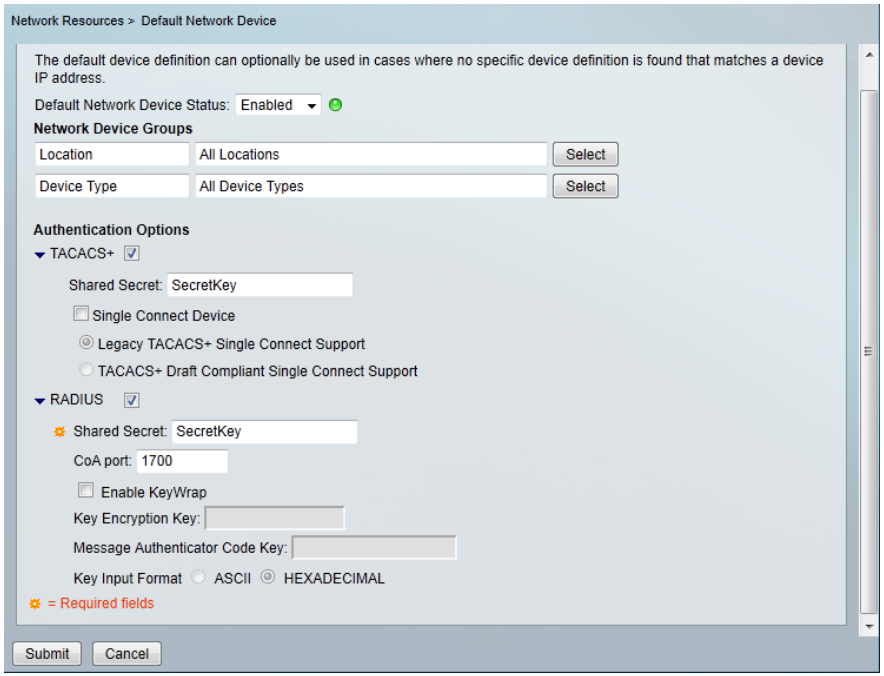
Step 1: Navigate to **Network Resources > Default Network Device**.

Step 2: In the Default Network Device Status list, choose **Enabled**.

Next, you must show the RADIUS configuration.

Step 3: Under Authentication Options, click the arrow next to **RADIUS**.

Step 4: In the Shared Secret box, type the secret key that is configured on the organization's access points, and then click **Submit**. (Example: SecretKey)



Process

Configuring the RADIUS Server: Windows Server 2008

1. Install services

If you don't require a comprehensive AAA system that spans the entire organizations management and user access, a simple RADIUS server can be used as an alternative to Cisco ACS.

The following procedures describe the steps required to enable RADIUS authentication for the WLAN controller deployment in this guide on an existing Windows Server 2008 Enterprise Edition installation.

For information about configuring the RADIUS server on Cisco ACS, use the previous process instead.

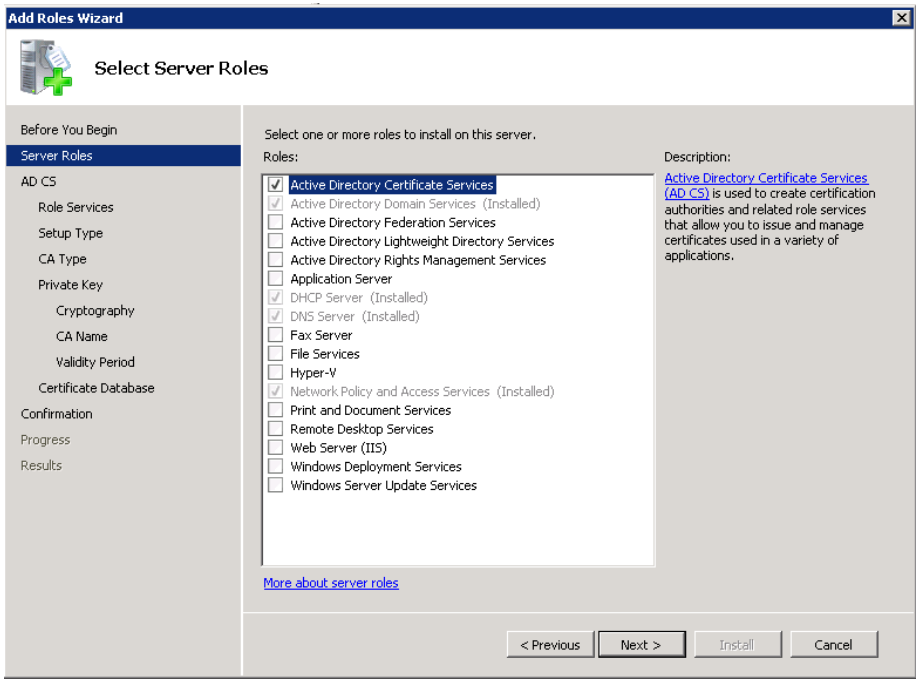
Procedure 1 Install services

Step 1: Join the server to your existing domain, and then restart.

Step 2: After the server restarts, open Server Manager.

Step 3: Navigate to **Roles >Add Roles.**

Step 4: On the Server Roles page, select **Active Directory Certificate Services** and **Network Policy and Access Services**, and then click **Next**.



Step 5: Follow the instructions in the wizard. Note the following:

- When configuring the Network Policy and Access Services role, select **Network Policy Server** and leave the default Certification Authority role service selected for AD CS.
- For the setup type for Active Directory CS, choose **Enterprise**.
- For the CA Type, choose **Root CA**.

Tech Tip

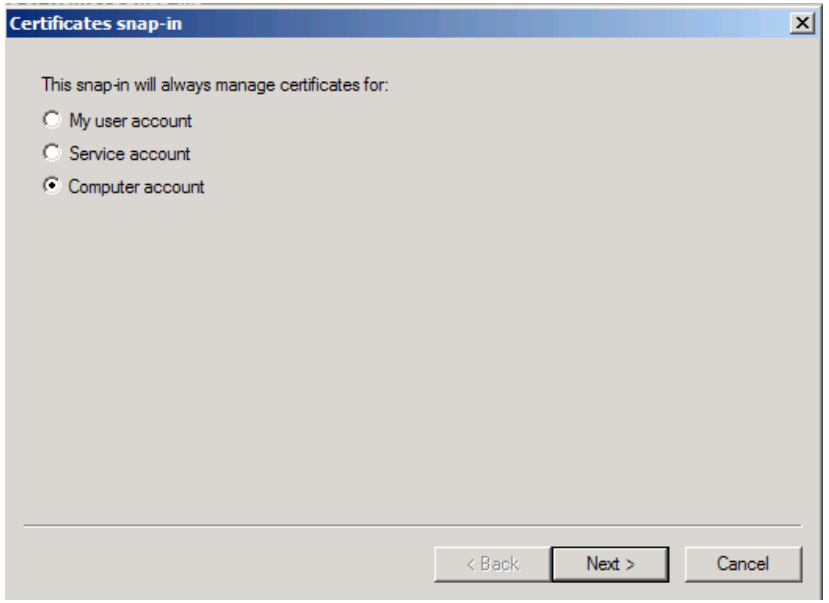
We're assuming that this is the first certificate authority (CA) in your environment. If it's not, you either don't need to install this role or you can configure this server as a subordinate CA instead.

Follow the rest of the instructions in the wizard, making any changes you want or just leaving the default values as appropriate. Note that there is a warning at the end of the wizard, stating that the name of this server cannot be changed after installing the AD CS role.

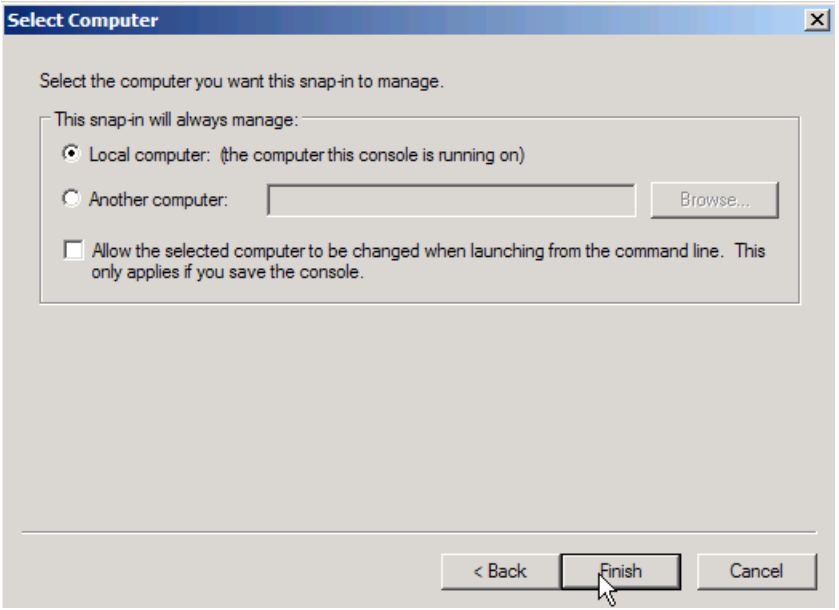
Now that you have a root CA and an NPS server on your domain, you can configure it.

Step 6: Open an MMC console, and then click **File -> Add/Remove Snap-in**.

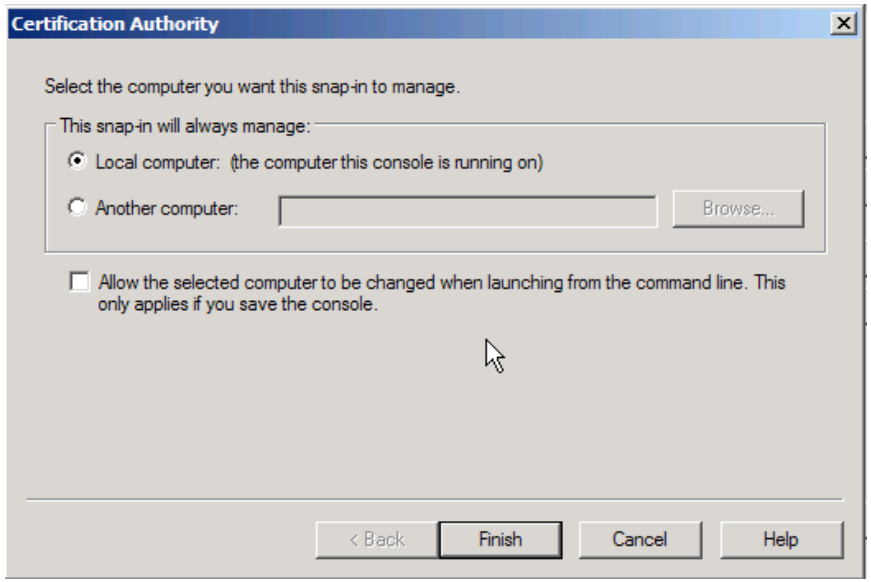
Step 7: In Certificates snap-in, select **Computer account**, and then click **Next**.



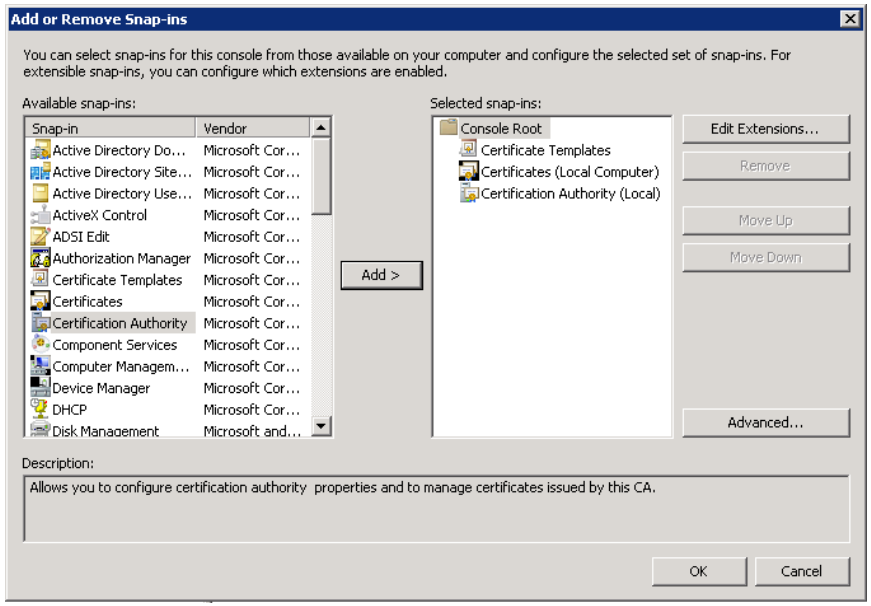
Step 8: In Select Computer, select **Local computer**, and then click **Finish**.



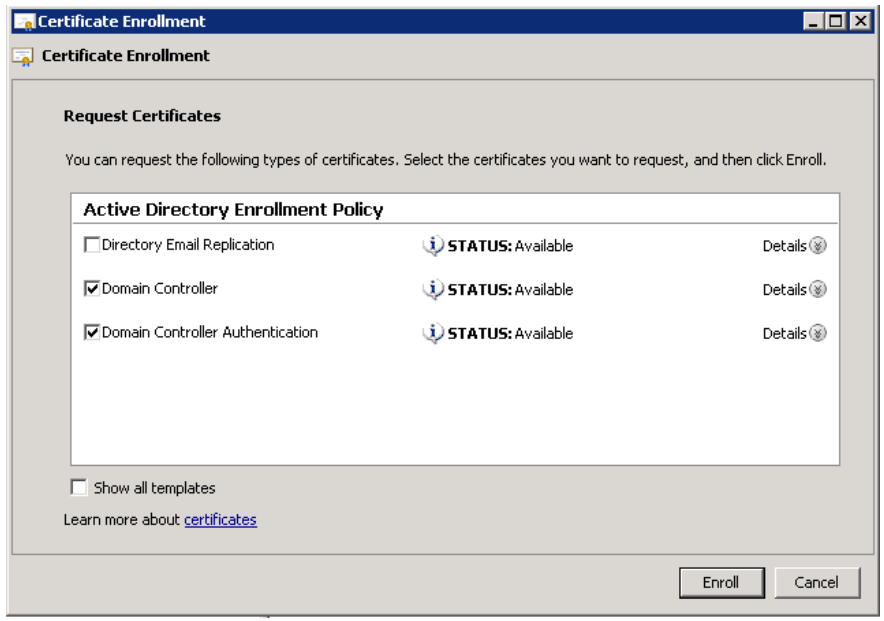
Step 9: Add the Certification Authority Snap-in.



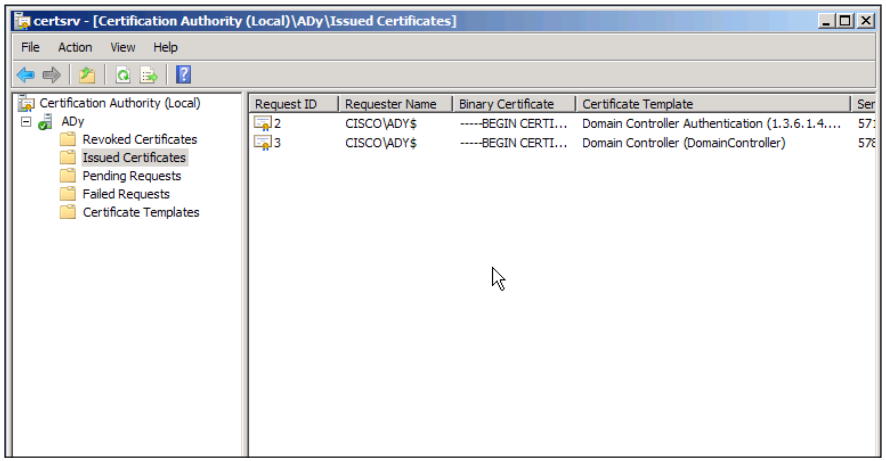
Step 10: Add the Certificate Templates Snap-in, and then click **OK**.



Step 11: Expand **Certificates (Local Computers) -> Personal**, right-click **Certificates**, and then click **Request new certificate**.

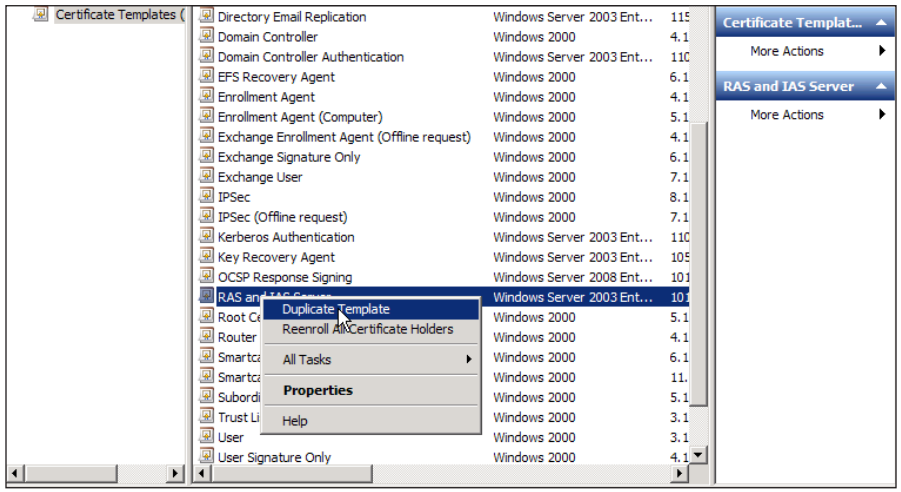


Step 12: Follow the instructions in the wizard, choosing **Computer** for the certificate type, and then click **Enroll**. Verify that the Certificate Templates folder appears under Certificate Authority / Issued Certificates.

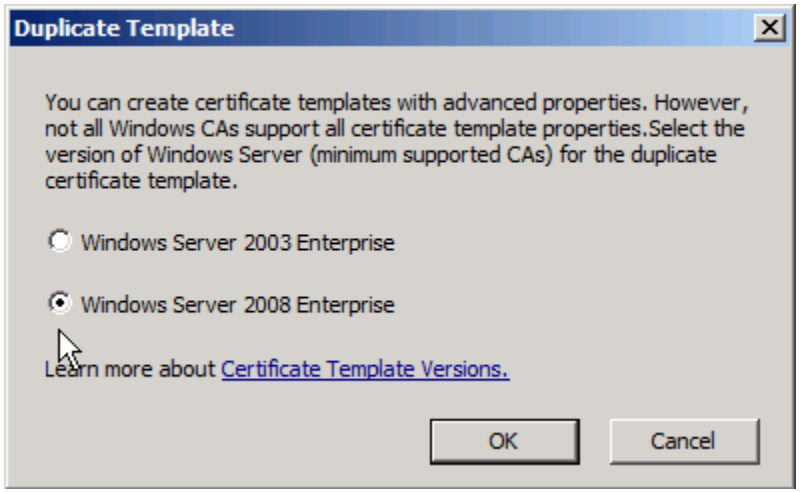


Step 13: Click the **Certificate Templates** folder, and in the right pane, locate **RAS and IAS Server**.

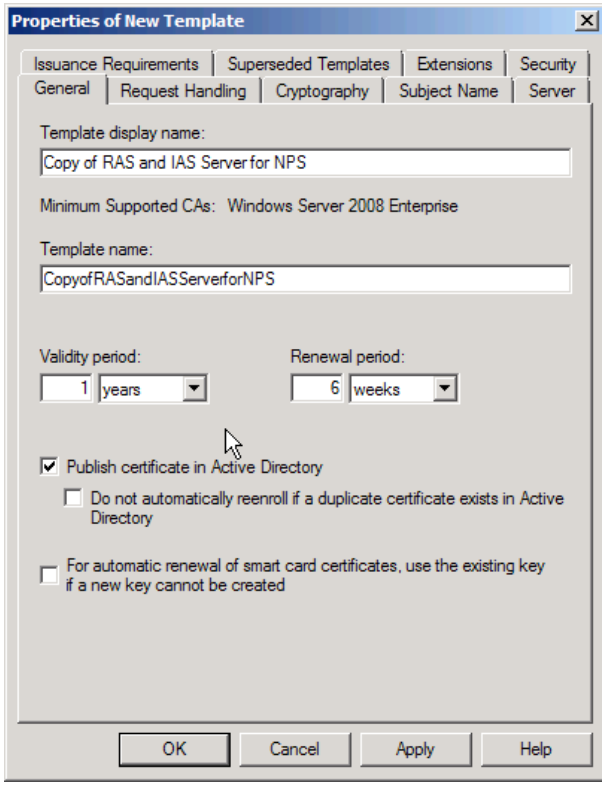
Step 14: Right-click **RAS and IAS Server**, and then click **Duplicate Template**.



Step 15: Select **Windows Server 2008 Enterprise**, and then click **OK**.

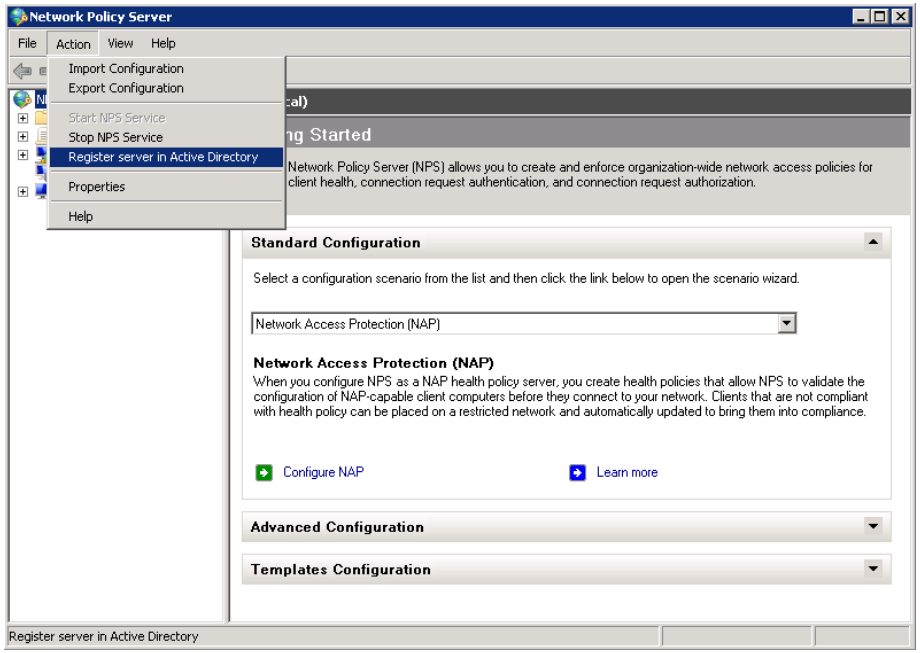


Step 16: Type a valid display name, select **Publish Certificate in Active Directory**, click **Apply**, and then close the MMC console.



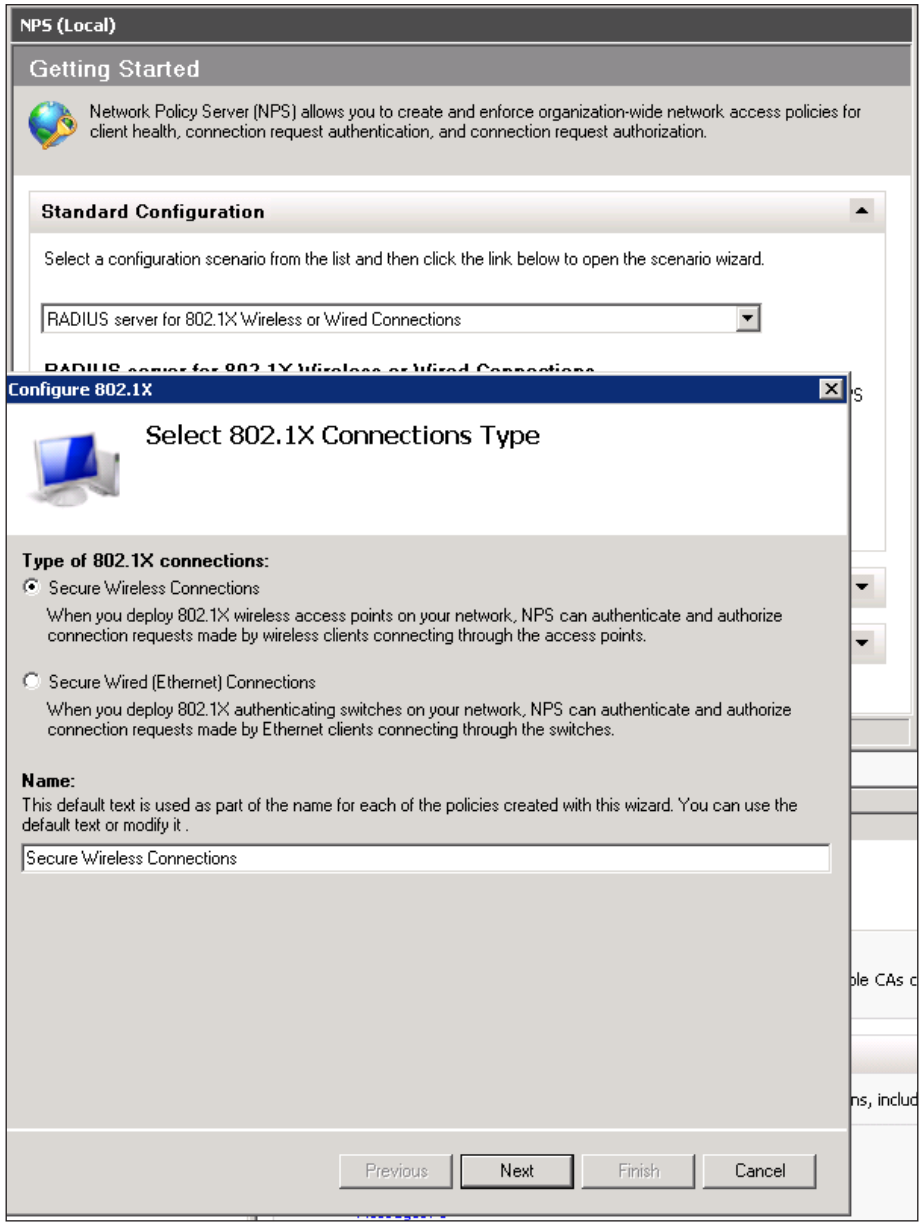
Step 17: From Administrative Tools, open the Network Policy Server administrative console.

Step 18: Right-click the parent node **NPS (Local)**, click **Register server in Active Directory**, click **OK**, and then click **OK** again.

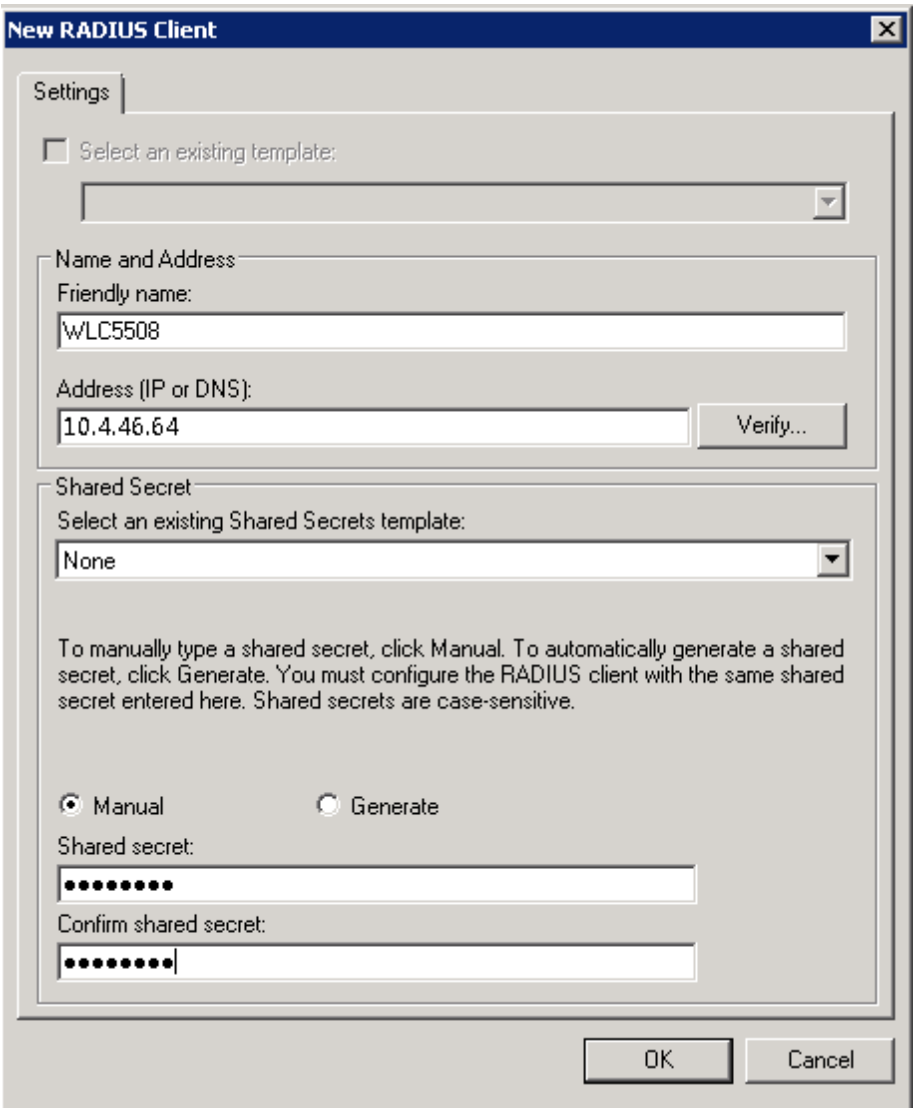


Step 19: With the NPS (Local) node still selected, select **RADIUS server for 802.1X Wireless or Wired Connections**, and then click **Configure 802.1X**.

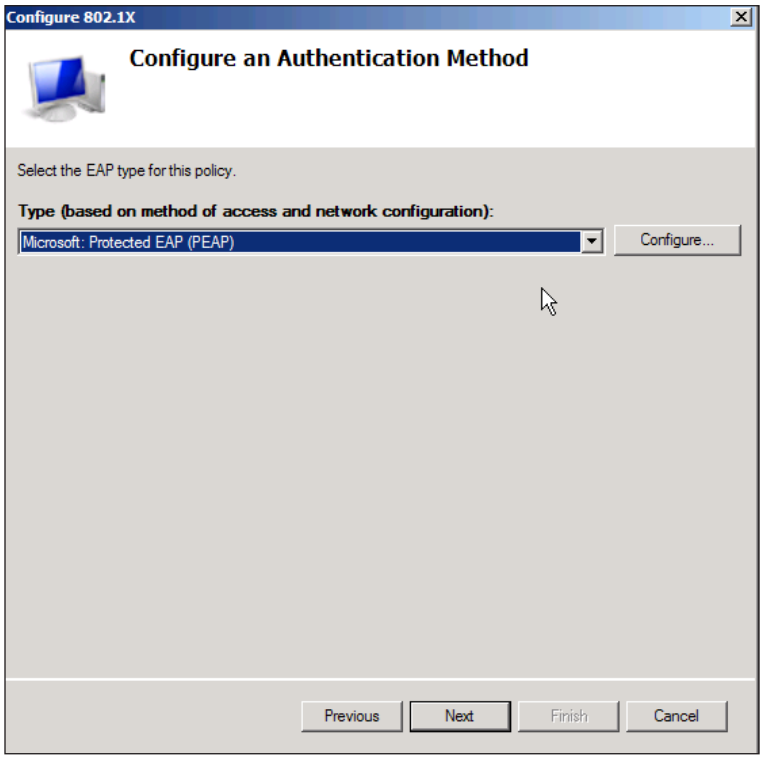
Step 20: Under Type of 802.1X connections, select **Secure Wireless Connections**, type an appropriate name for the policies that you want to create with this wizard, and then click **Add**.



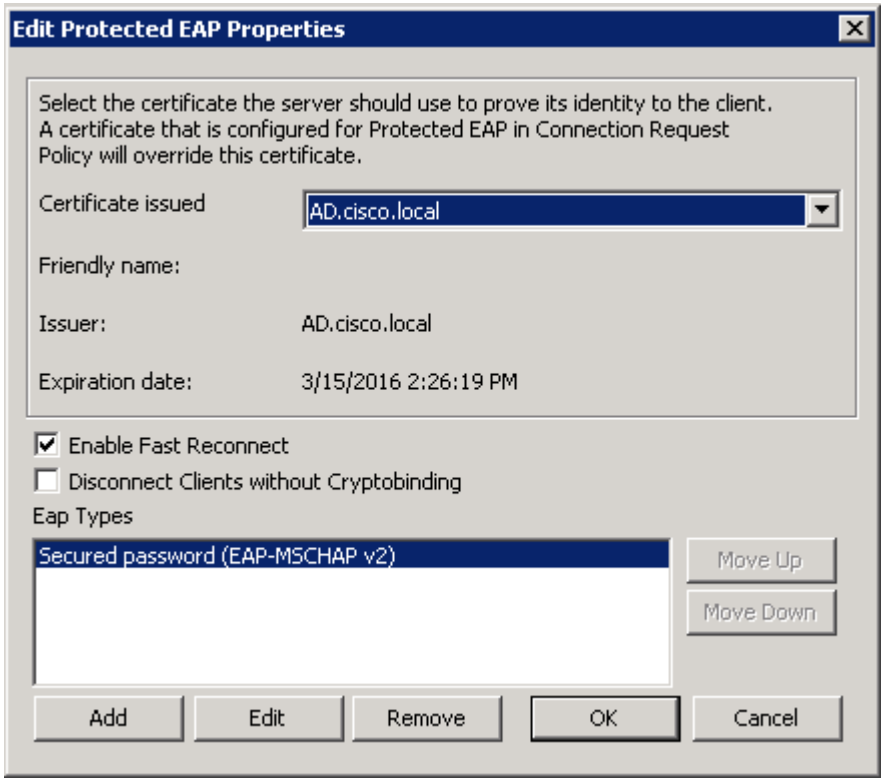
Step 21: In the **Friendly name** box, type a name for the controller (for example, WLC-1), and then provide the IP address or DNS entry for the controller.



Step 22: Click **Next**, select **Microsoft: Protected EAP (PEAP)**, and then click **Configure**. .

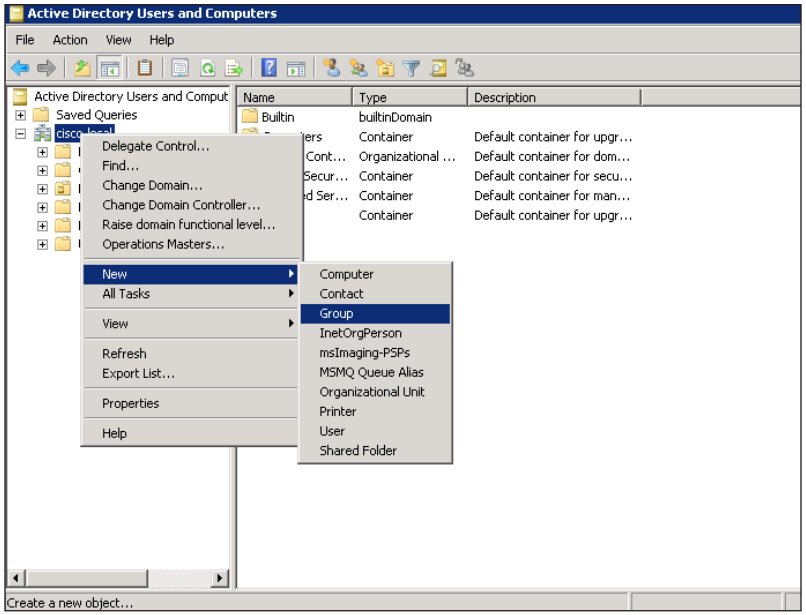


Step 23: Ensure that the Certificate issued drop-down list box displays the certificate you enrolled in Step 11.

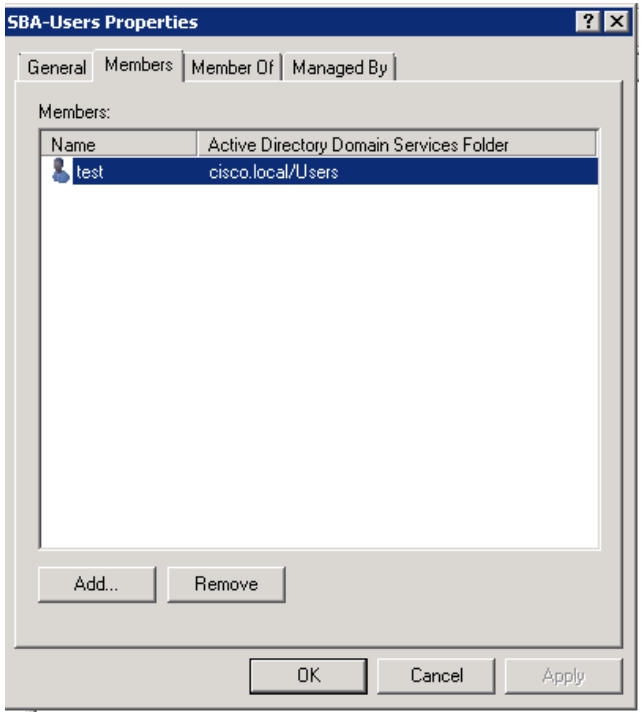


Step 24: In Specify User Groups, click **Add** to add a group that you already created, or perform the following steps to create a group and add users to the group.

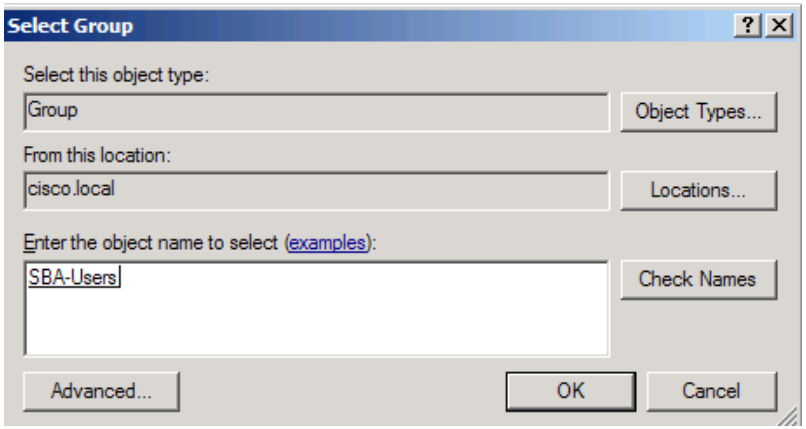
Step 25: Create a group called SBA-Users.



Step 26: Create a user named **test** and add it to the group created in the previous step.

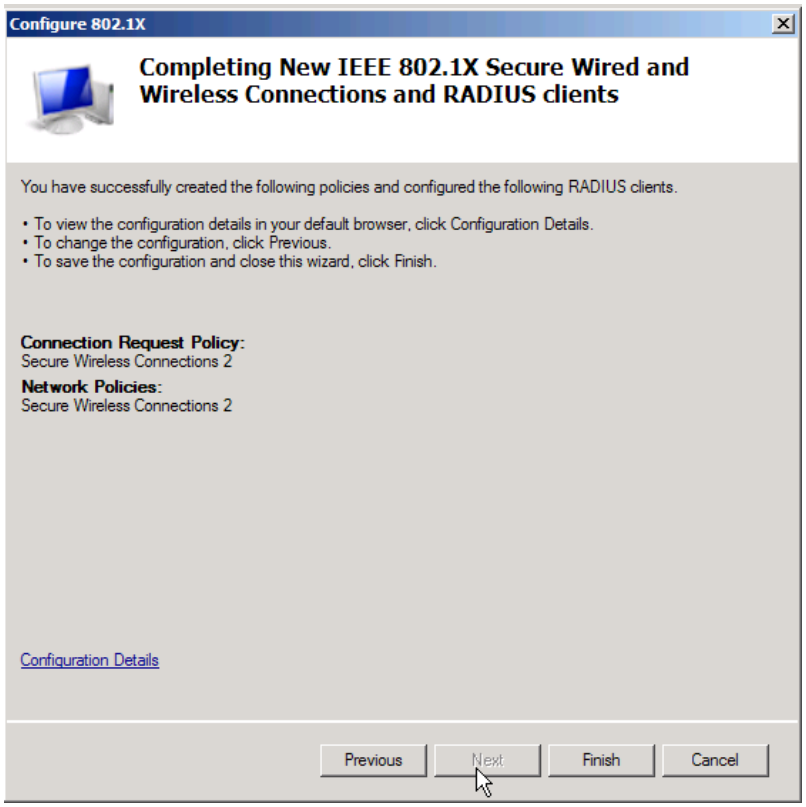


Step 27: Click **Next**, and then click **Add** to use an Active Directory group to secure your wireless (you should add both the machine accounts and user accounts to this group to allow the machine to authenticate on the wireless before the user logs in).



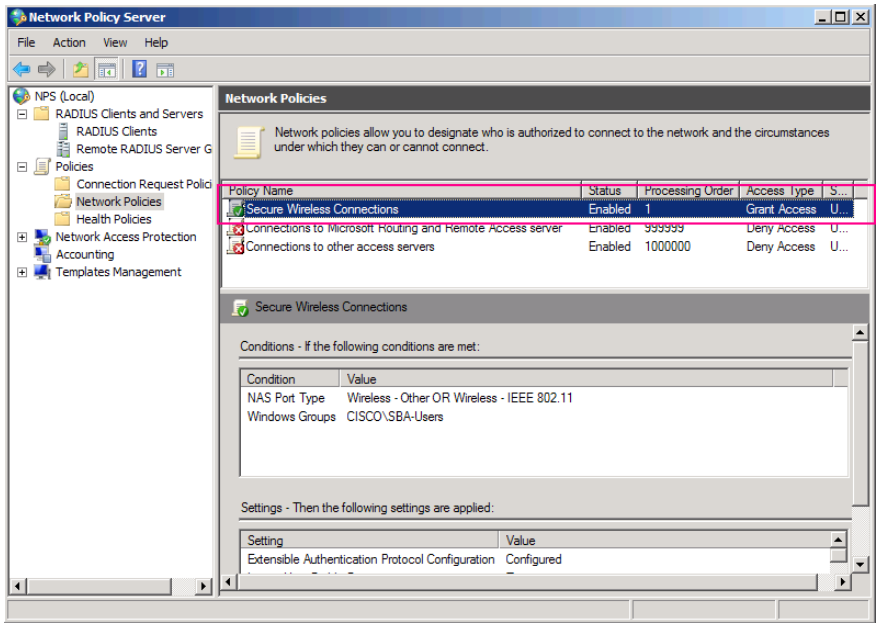
Step 28: On the next step of the wizard, you can configure VLAN information or just accept the default settings.

Step 29: Click **Finish**. This completes the configuration of 802.1x.



Step 30: Restart the Network Policy Server service.

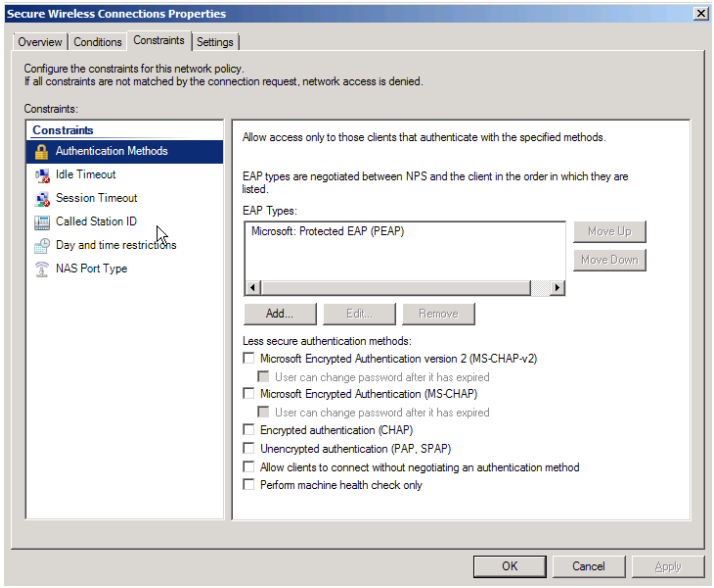
If you expand the Policies node now, you'll see that the wizard has created a Connection Request Policy and a Network Policy containing the appropriate settings to authenticate your wireless connection – You can create these individual policies manually, but the wizard is an easier method.



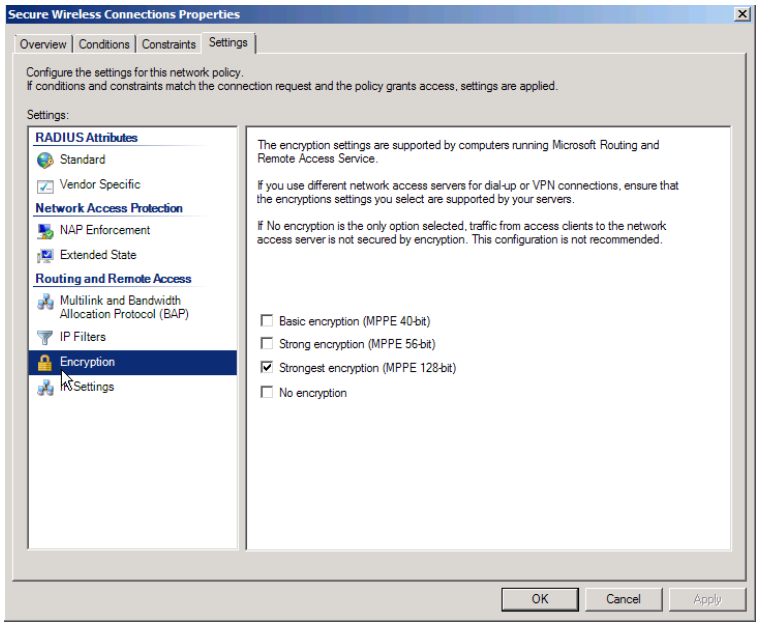
You can also remove the less secure authentication method options and increase the encryption methods in the network policy if you want.

Step 31: Under the Network Policies node, open the properties of the newly created policy.

Step 32: On the Constraints tab, clear all of the check boxes under **Less secure authentication methods**.



Step 33: On the Settings tab, click **Encryption**, and clear all check boxes except **Strongest encryption (MPPE 128-bit)**.



Step 34: Save the policy, and then restart the Network Policy Server service.

Process

Configuring On-Site Wireless Controllers with Local-Mode

1. Configure the switch for the controller
2. Configure the WLC platform
3. Configure the time zone
4. Configure SNMP
5. Limit what networks can manage the WLC
6. Configure wireless user authentication
7. Configure management Authentication
8. Create the WLAN data interface
9. Create the wireless LAN voice interface
10. Configure the data wireless LAN
11. Configure the voice wireless LAN
12. Configure the resilient controller
13. Configure mobility groups
14. Configure controller discovery
15. Connect the access points
16. Configure access points for resiliency

In a local-mode deployment, the wireless LAN controller and access points are co-located at the same site. The wireless LAN controller is connected to a LAN distribution layer at the site, and traffic between wireless LAN clients and the LAN is tunneled in Control and Provisioning of Wireless Access Points (CAPWAP) protocol between the controller and the access point.

Table 2 - Cisco on-site wireless controller parameters checklist

Parameter	Cisco SBA values primary controller	Cisco SBA values resilient controller	Site-specific values
Controller parameters			
Switch Interface Number	1/0/3, 2/0/3	1/0/4, 2/0/4	
VLAN number	146		
Time zone	PST -8 0		
IP address	10.4.46.64/24	10.4.46.65/24	
Default gateway	10.4.46.1		
Hostname	WLC-1	WLC-2	
Mobility group name	CAMPUS		
RADIUS server IP address	10.4.48.15		
RADIUS shared key	SecretKey		
Management network (optional)	10.4.48.0/24		
TACACS server IP address (optional)	10.4.48.15		
TACACS shared key (optional)	SecretKey		
Wireless data network parameters			
SSID	WLAN-Data		
VLAN number	116		
Default gateway	10.4.16.1		
Controller interface IP address	10.4.16.5/22	10.4.16.6/22	
Wireless voice network parameters			
SSID	WLAN-Voice		
VLAN number	120		
Default gateway	10.4.20.1		
Controller interface IP address	10.4.20.5/22	10.4.20.6/22	

Procedure 1 Configure the switch for the controller

Step 1: On the LAN distribution switch, create the wireless VLANs that you are connecting to the distribution switch. The management VLAN can contain other Cisco appliances and does not have to be dedicated to the WLCs.

```
vlan 116
 name WLAN_Data
vlan 120
 name WLAN_Voice
vlan 146
 name WLAN_Mgmt
```

Step 2: Configure a VLAN interface (SVI) for each VLAN so devices in the VLAN can communicate with the rest of the network.

```
interface Vlan116
 description Wireless Data Network
 ip address 10.4.16.1 255.255.252.0
 no shutdown
!
interface Vlan120
 description Wireless Voice Network
 ip address 10.4.20.1 255.255.252.0
 no shutdown
!
interface Vlan146
 description Wireless Management Network
 ip address 10.4.46.1 255.255.255.0
 no shutdown
```

Step 3: For interface configuration, an 802.1Q trunk is used for the connection to the WLCs. This allows the distribution switch to provide the Layer 3 services to all the networks defined on the WLC. The VLANs allowed on the trunk are limited to only the VLANs that are active on the WLC.

If you are deploying the Catalyst 4500 LAN distribution switch, you do not need to use the **switchport trunk encapsulation dot1q** command in the following configurations.

If you are deploying a Cisco 5500 Series Wireless LAN Controller, configure at least two distribution switch interfaces as an EtherChannel trunk.

```
interface GigabitEthernet [port 1]
 description To WLC Port 1
interface GigabitEthernet [port 2]
 description To WLC Port 2
!
interface range GigabitEthernet [port 1], GigabitEthernet
[port 2]
  switchport
  macro apply EgressQoS
  channel-group [number] mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
!
interface Port-channel [number]
 description To WLC
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 116,120,146
 switchport mode trunk
 logging event link-status
 no shutdown
```

If you are deploying a Cisco 2500 Series Wireless LAN Controller, configure a single distribution switch interface as a trunk.

```
interface GigabitEthernet [port]
 description To WLC Port 1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 116,120,146
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

Procedure 2 Configure the WLC platform

After the WLC is physically installed and powered up, you will see the following on the console:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: YES
```

Step 1: Enter a system name. (Example: WLC-1)

```
System Name [Cisco_7e:8e:43] (31 characters max): WLC-1
```

Step 2: Enter an administrator username and password.

Tech Tip

Use at least three of the following four classes in the password: lowercase letters, uppercase letters, digits, or special characters.

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****
```

Step 3: If you are deploying a Cisco 5500 Series Wireless LAN Controller, use DHCP for the service port interface address.

```
Service Interface IP address Configuration [none] [DHCP]: DHCP
```

Step 4: Enable the management interface.

If you are deploying a Cisco 5500 Series Wireless LAN Controller, configure at least two interfaces as an EtherChannel trunk.

```
Enable Link Aggregation (LAG) [yes][NO]: YES
Management Interface IP Address: 10.4.46.64
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.46.1
Management Interface VLAN Identifier (0 = untagged): 146
```

If you are deploying a Cisco 2500 Series Wireless LAN Controller, configure a single interface as a trunk.

```
Management Interface IP Address: 10.4.46.64
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.46.1
Management Interface VLAN Identifier (0 = untagged): 146
Management Interface Port Num [1 to 4]: 1
```

Step 5: Enter the default DHCP server for clients. (Example: 10.4.48.10)

```
Management Interface DHCP Server IP Address: 10.4.48.10
```

Step 6: The virtual interface is used by the WLC for Mobility DHCP relay and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

```
Virtual Gateway IP Address: 192.0.2.1
```

Step 7: Enter a name that will be used as the default mobility and RF group. (Example: CAMPUS)

```
Mobility/RF Group Name: CAMPUS
```

Step 8: Enter an SSID for the WLAN that supports data traffic. You will be able to leverage this later in the deployment process.

```
Network Name (SSID): WLAN-Data
Configure DHCP Bridging Mode [yes][NO]: NO
```

Step 9: For increased security, enable DHCP snooping.

```
Allow Static IP Addresses {YES][no]: NO
```

Step 10: You will configure the RADIUS server later by using the GUI.

```
Configure a RADIUS Server now? [YES][no]: NO
```

Step 11: Enter the correct country code for the country where you are deploying the WLC.

```
Enter Country Code list (enter 'help' for a list of countries)
[US]: US
```

Step 12: Enable all wireless networks.

```
Enable 802.11b network [YES][no]: YES
Enable 802.11a network [YES][no]: YES
Enable 802.11g network [YES][no]: YES
```

Step 13: Enable the radio resource management (RRM) auto-RF feature. This helps you keep your network up and operational.

```
Enable Auto-RF [YES][no]: YES
```

Step 14: Synchronize the WLC clock to your organization's NTP server.

```
Configure a NTP server now? [YES][no]:YES
Enter the NTP server's IP address: 10.4.48.17
Enter a polling interval between 3600 and 604800 secs: 86400
```

Step 15: Save the configuration. If you respond with **no**, the system restarts without saving the configuration and you have to complete this procedure again.

```
Configuration correct? If yes, system will save it and reset.
[yes][NO]: YES
Configuration saved!
Resetting system with new configuration
```

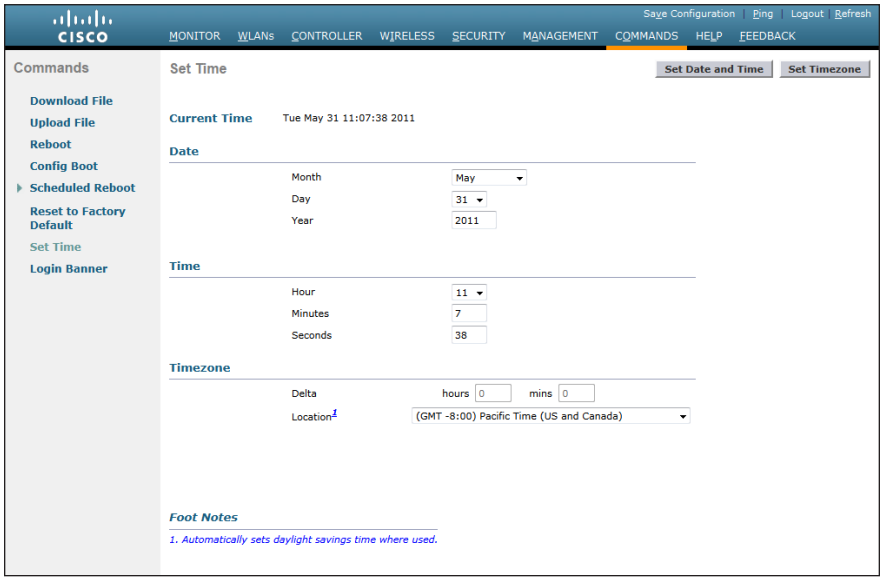
Step 16: After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page using the credentials defined in Step 2. (Example: https://wlc-1.cisco.local/)

Procedure 3 Configure the time zone

Step 1: Navigate to **Commands** > **Set Time.**

Step 2: In the Location list, choose the time zone that corresponds to the location of the WLC.

Step 3: Click **Set Timezone**.



Procedure 4 Configure SNMP

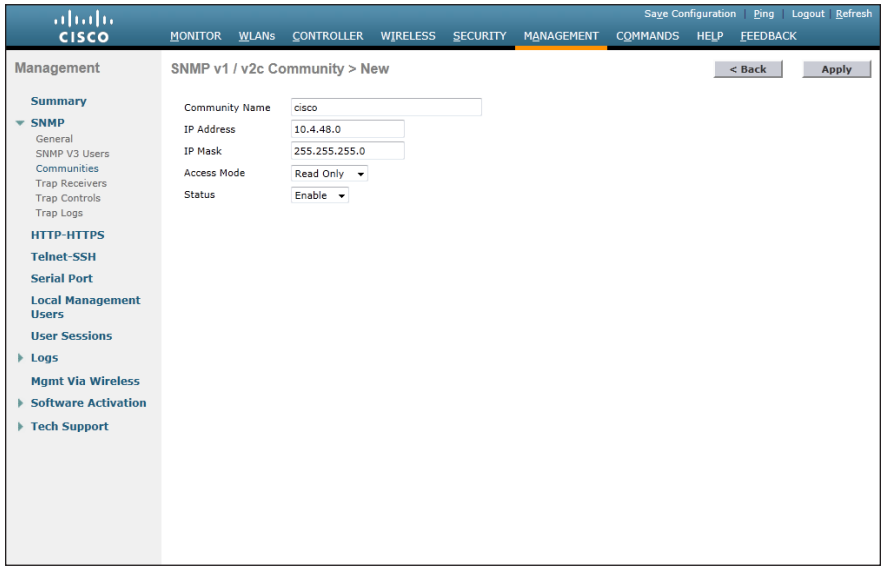
Step 1: In **Management** > **SNMP** > **Communities**, click **New**.

Step 2: Enter the **Community Name**. (Example: cisco)

Step 3: Enter the **IP Address.** (Example: 10.4.48.0)

Step 4: Enter the **IP Mask**. (Example: 255.255.255.0)

Step 5: In the Status list, choose **Enable**., and then click **Apply**.



Step 6: In **Management** > **SNMP** > **Communities**, click **New**.

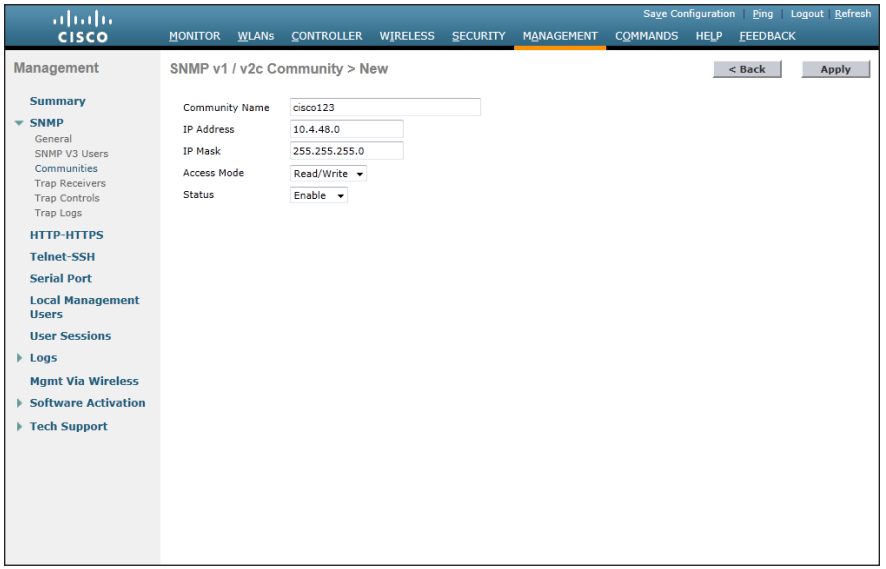
Step 7: Enter the **Community Name**. (Example: cisco123)

Step 8: Enter the **IP Address.** (Example: 10.4.48.0)

Step 9: Enter the **IP Mask**. (Example: 255.255.255.0)

Step 10: In the Access Mode list, choose **Read/Write**.

Step 11: In the Status list, choose **Enable**, and then click **Apply**.

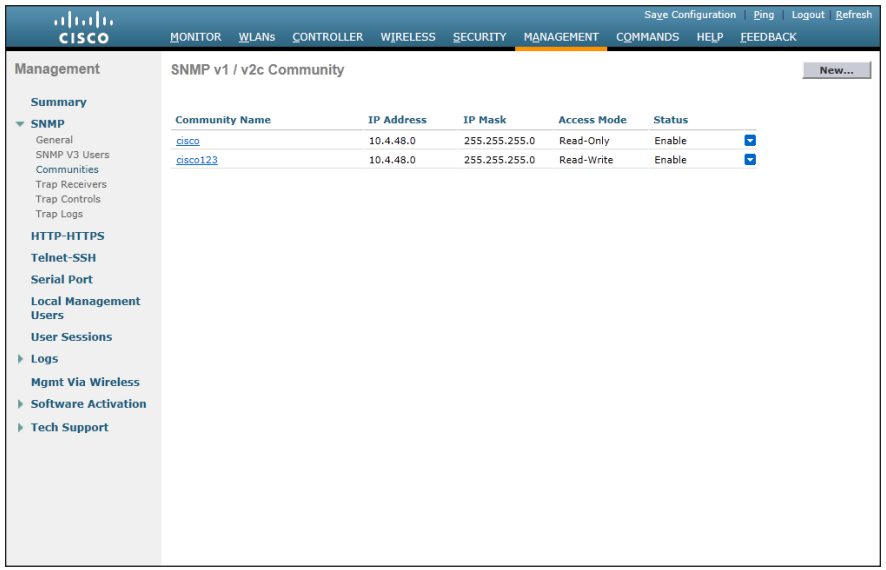


Step 12: Navigate to **Management** > **SNMP** > **Communities**.

Step 13: Point to the blue box for the **public** community, and then click **Remove**.

Step 14: On the message "Are you sure you want to delete?", click **OK**.

Step 15: Repeat Step 13 and Step 14 for the **private** community.



Procedure 5 Limit what networks can manage the WLC

(Optional)

In networks where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your controller. In this example, only devices on the 10.4.48.0/24 network will be able to access the controller via Secure Shell (SSH) Protocol or Simple Network Management Protocol (SNMP).

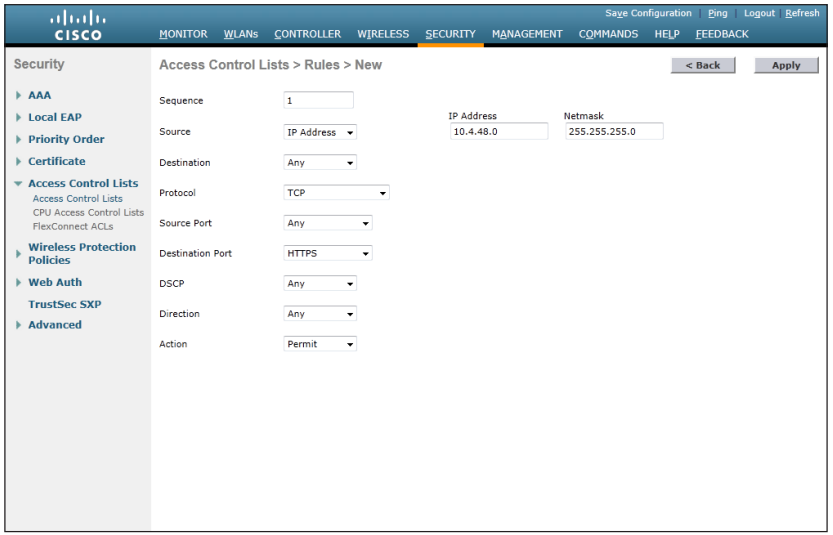
Step 1: In **Security** > **Access Control Lists** > **Access Control Lists**, click **New**.

Step 2: Enter an access list name, and then click **Apply**.

Step 3: In the list, choose the name of the access list you just created, and then click **Add New Rule**.

Step 4: In the window, enter the following configuration details, and then click **Apply**.

- Sequence—1
- Source—10.4.48.0 / 255.255.255.0
- Destination—Any
- Protocol—TCP
- Destination Port—HTTPS
- Action—Permit



Step 5: Repeat Step 1 through Step 4 four more times, using the configuration details in the following table.

Sequence	Source	Destination	Protocol	Destination port	Action
2	10.4.48.0/ 255.255.255.0	Any	TCP	Other/22	Permit
3	Any	Any	TCP	HTTPS	Deny
4	Any	Any	TCP	Other/22	Deny
5	Any	Any	Any	Any	Permit

Step 6: In **Security > Access Control Lists > CPU Access Control Lists**, select **Enable CPU ACL**.

Step 7: In the **ACL Name** list, choose the ACL you created in Step 2, and then click **Apply.**

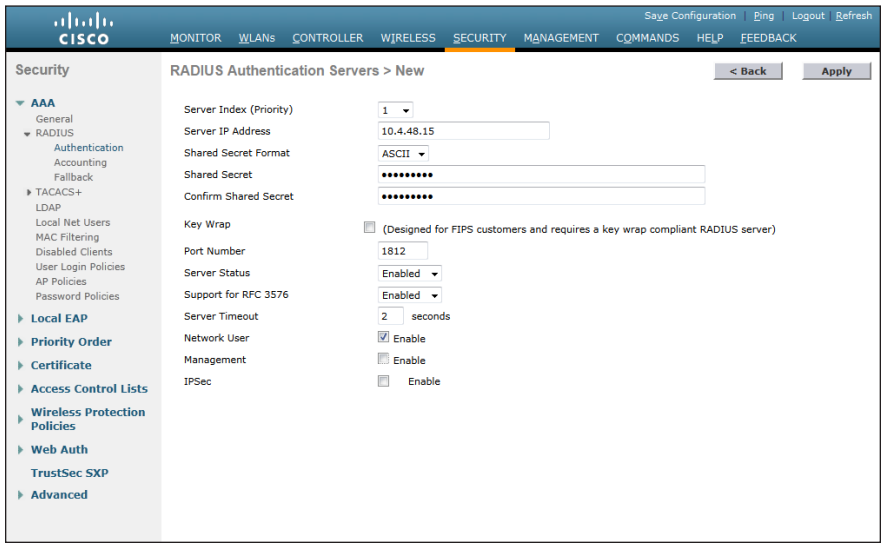
Procedure 6 Configure wireless user authentication

Step 1: In **Security > AAA > Radius > Authentication**, click **New**.

Step 2: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 3: Enter and confirm the **Shared Secret**. (Example: SecretKey)

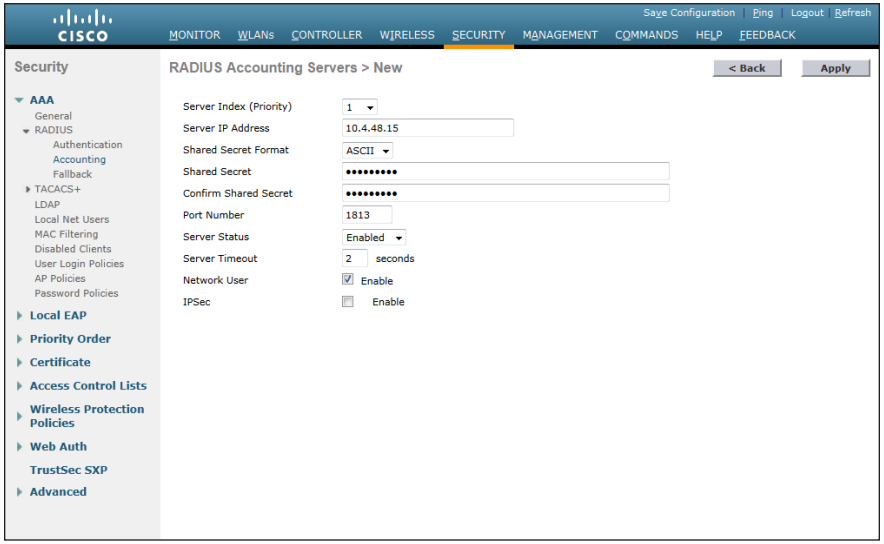
Step 4: To the right of Management, clear **Enable**, and then click **Apply**.



Step 5: In **Security > AAA > Radius > Accounting**, click **New**.

Step 6: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 7: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



Procedure 7 Configure management Authentication

(Optional)

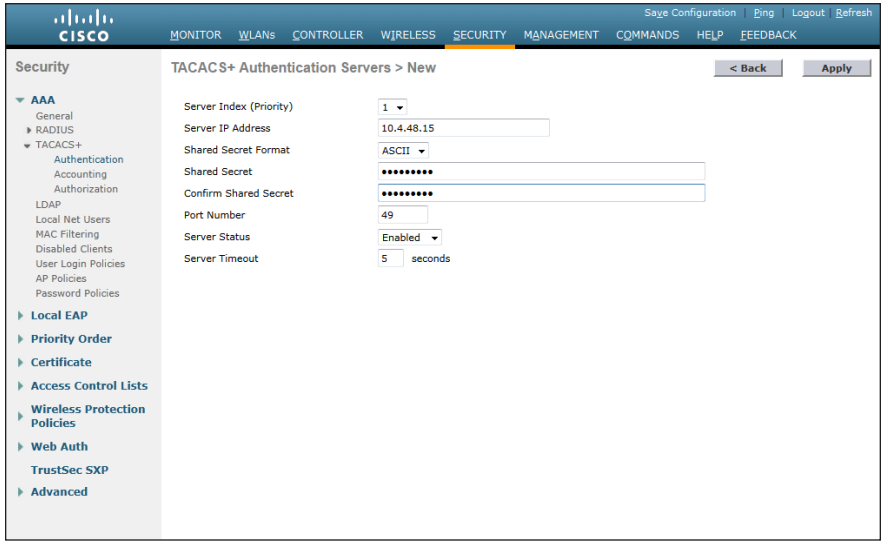
You can use this procedure to deploy centralized management authentication by configuring the Authentication, Authorization and Accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 8.

As networks scale in the number of devices to maintain, the operational burden to maintain local management accounts on every device also scales. A centralized Authentication, Authorization and Accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

Step 1: In **Security > AAA > TACACS+ > Authentication**, click **New**.

Step 2: Enter the **Server IP Address**. (Example: 10.4.48.15)

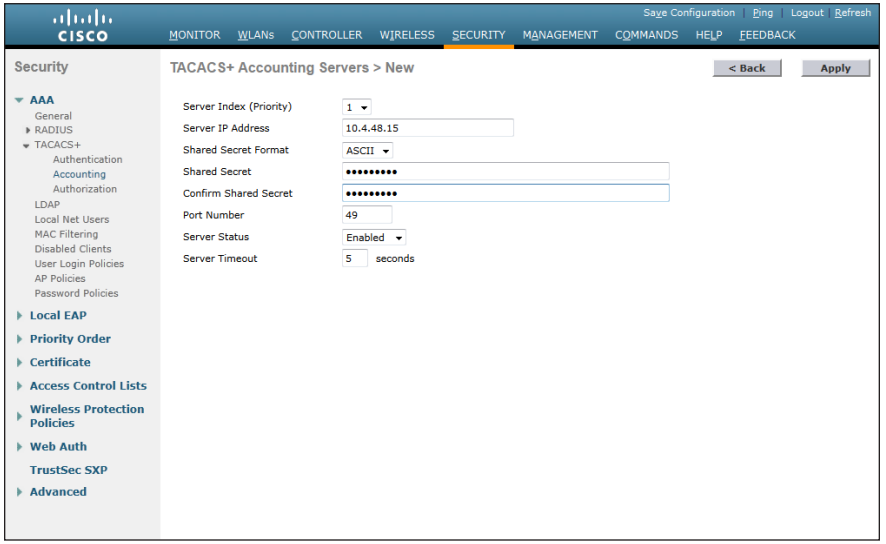
Step 3: Enter and confirm the **Shared Secret**, and then click **Apply** (Example: SecretKey)



Step 4: In **Security** > **AAA** > **TACACS+** > **Accounting**, click **New**.

Step 5: Enter the **Server IP Address**. (Example: 10.4.48.15)

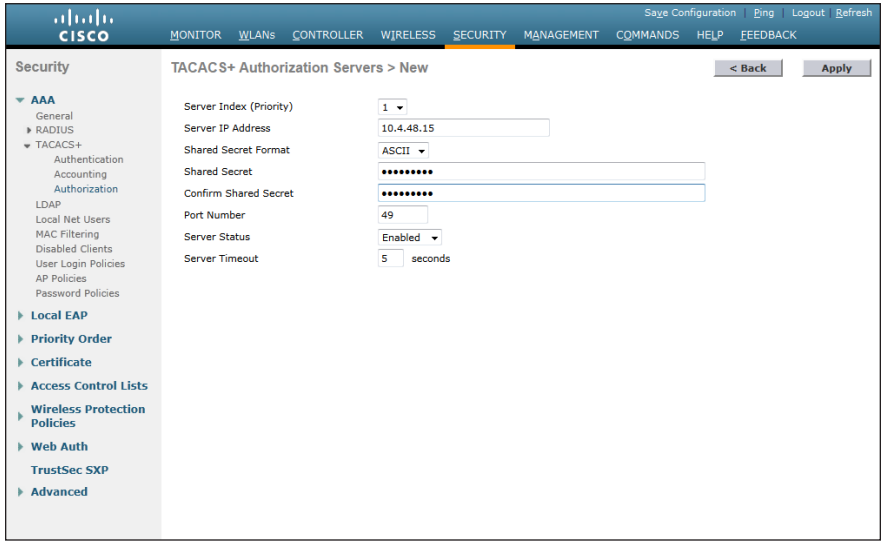
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



Step 7: In **Security** > **AAA** > **TACACS+** > **Authorization**, click **New**.

Step 8: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 9: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

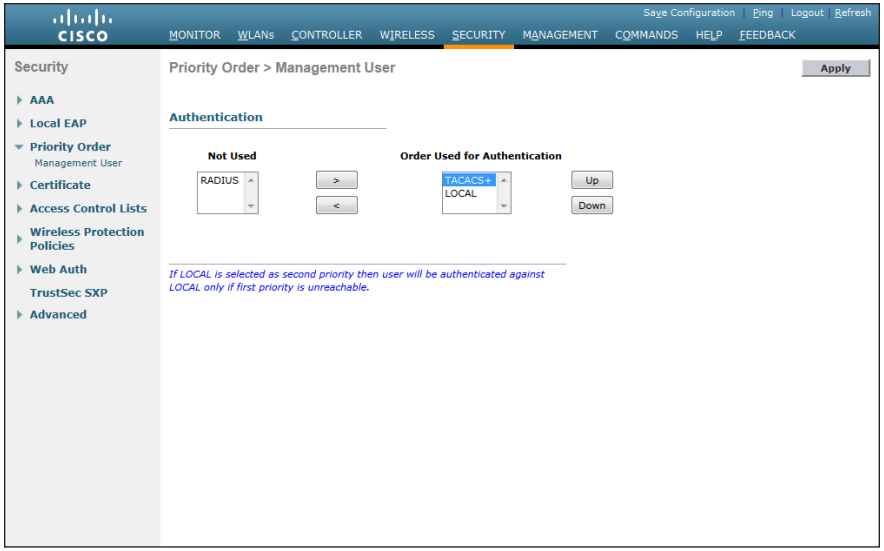


Step 10: Navigate to **Security > Priority Order > Management User.**

Step 11: Using the arrow buttons, move TACACS+ from the **Not Used** list to the **Used for Authentication** list.

Step 12: Using the **Up** and **Down** buttons, move TACACS+ to be the first in the **Order Used for Authentication** list.

Step 13: Using the arrow buttons, move RADIUS to the **Not Used** list, and then click **Apply**.



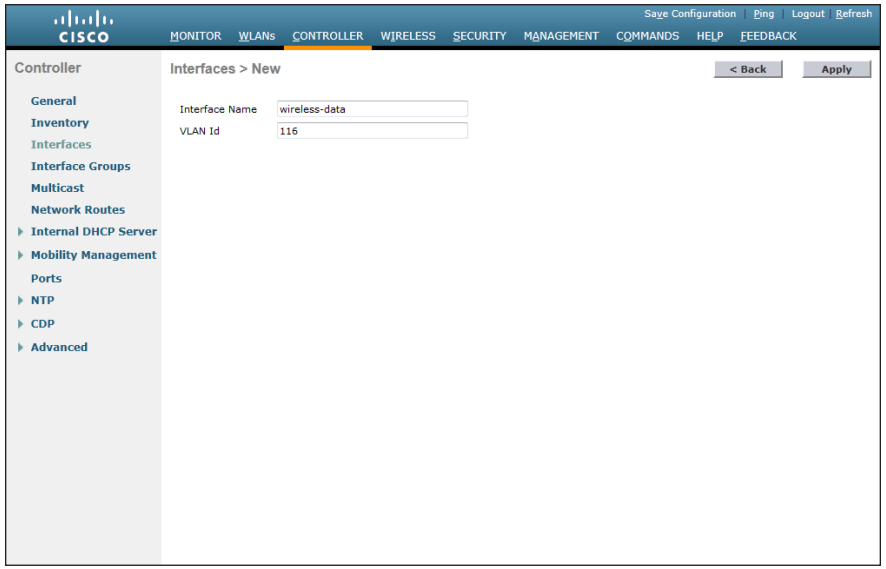
Procedure 8 Create the WLAN data interface

Configure the WLC to separate voice and data traffic, which is essential in any good network design in order to ensure proper treatment of the respective IP traffic, regardless of the medium it is traversing. In this procedure, you add an interface that allows devices on the wireless data network to communicate with the rest of your organization.

Step 1: In **Controller>Interfaces,** click **New**.

Step 2: Enter the **Interface Name**. (Example: Wireless-Data)

Step 3: Enter the **VLAN Id**, and then click **Apply**. (Example: 116)



Step 4: If you are deploying a Cisco 2500 Series Wireless LAN Controller, in the **Port Number** box, enter the port that is connected to the LAN distribution switch. (Example: 1)

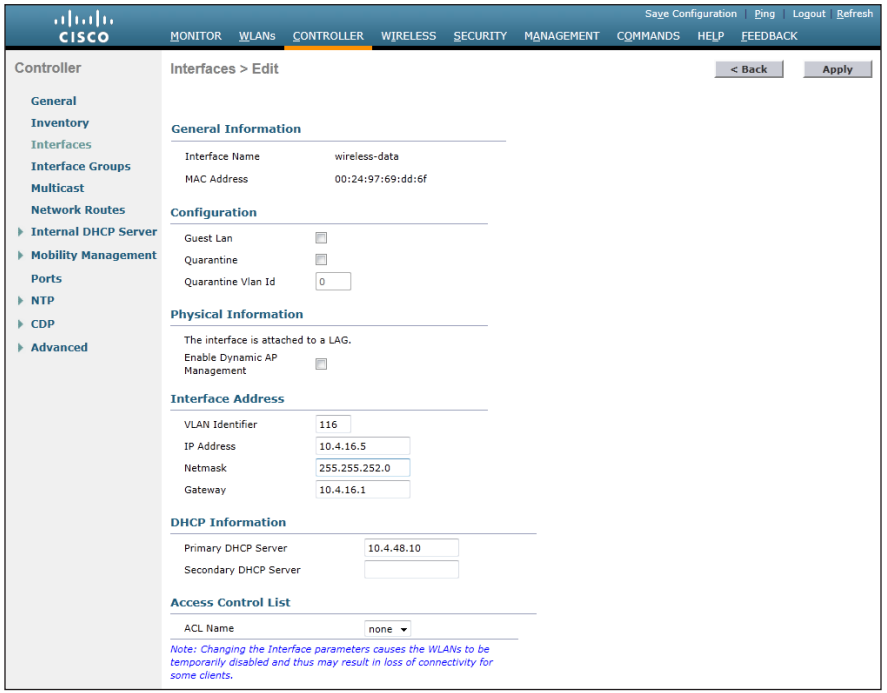
Step 5: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.16.5)

Step 6: Enter the **Netmask**. (Example: 255.255.252.0)

Step 7: In the **Gateway** box, enter the IP address of the VLAN interface defined in Procedure 1. (Example: 10.4.16.1)

Step 8: In the **Primary DHCP Server** box, enter the IP address of your organization's DHCP server. (Example: 10.4.48.10)

Step 9: Click **Apply**.



Tech Tip

To prevent DHCP from assigning addresses to wireless clients that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

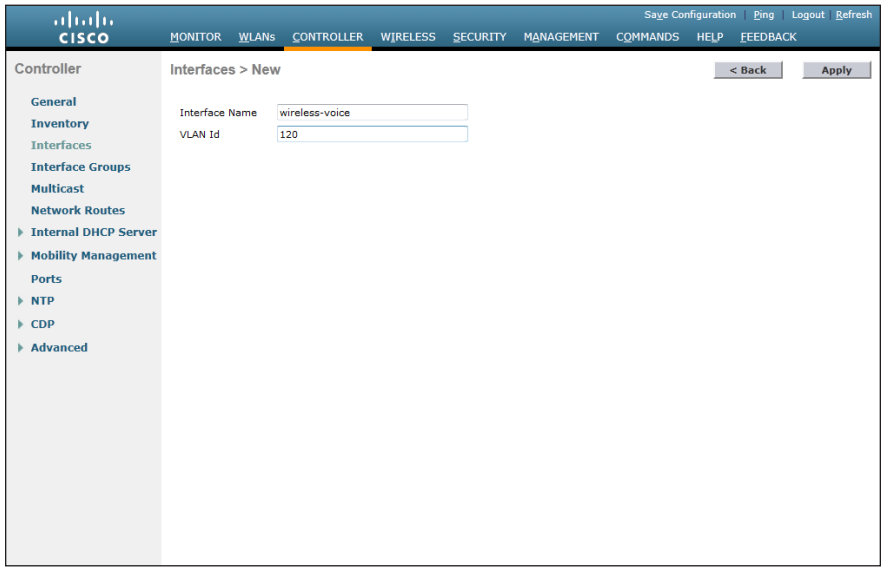
Procedure 9 Create the wireless LAN voice interface

You must add an interface that allows devices on the wireless voice network to communicate with the rest of the organization.

Step 1: In **Controller>Interfaces,** click **New**.

Step 2: Enter the **Interface Name**. (Example: wireless-voice)

Step 3: Enter the **VLAN Id**, and then click **Apply**. (Example: 120)



Step 4: If you are deploying a Cisco 2500 Series Wireless LAN Controller, in the **Port Number** box, enter the port that is connected to the LAN distribution switch. (Example: 1)

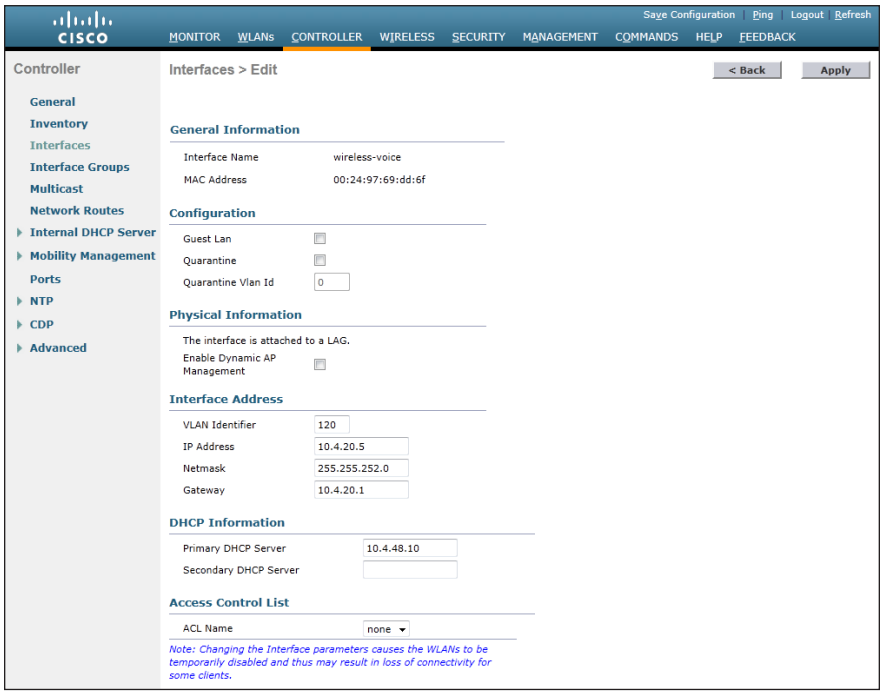
Step 5: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 10.4.20.5)

Step 6: Enter the **Netmask**. (Example: 255.255.252.0)

Step 7: In the **Gateway** box, enter the IP address of the VLAN interface defined in Procedure 1 (Example: 10.4.20.1)

Step 8: In the **Primary DHCP Server** box, enter the IP address of your organization's DHCP server. (Example: 10.4.48.10)

Step 9: Click **Apply**.



Tech Tip

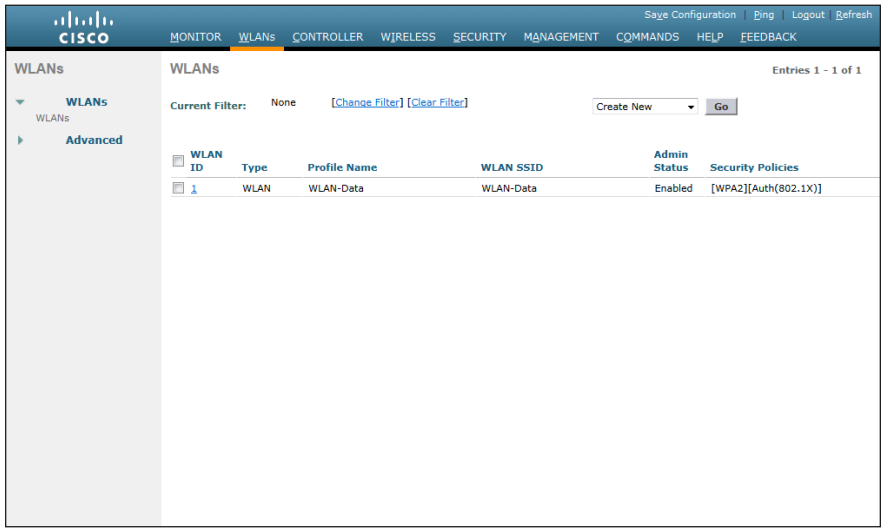
To prevent DHCP from assigning addresses to wireless clients that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Procedure 10 Configure the data wireless LAN

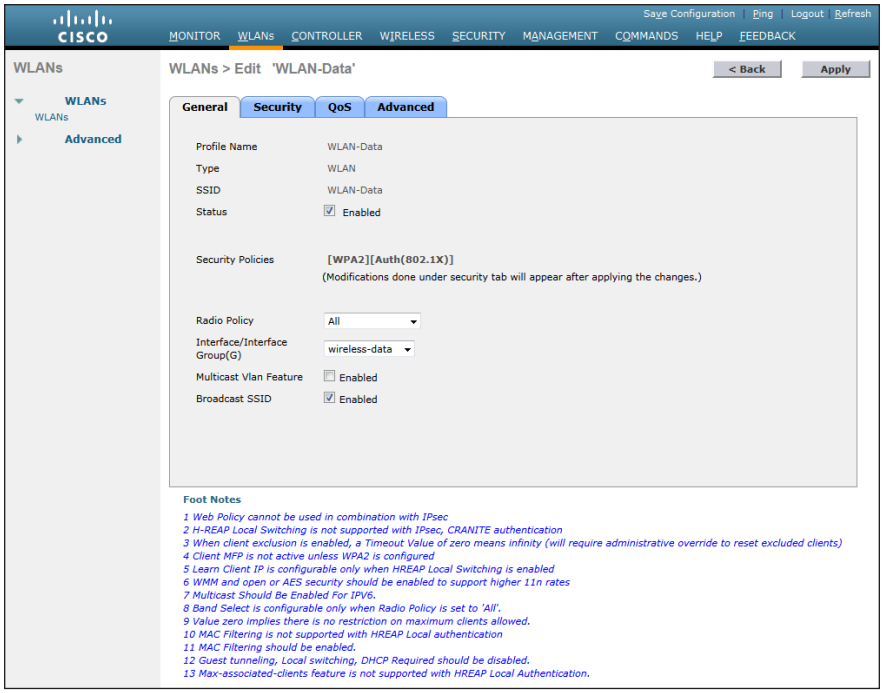
Wireless data traffic can handle delay, jitter, and packet loss more efficiently than wireless voice traffic.. For the data WLAN, keep the default QoS settings and segment the data traffic onto the data wired VLAN.

Step 1: Navigate to **WLANs**.

Step 2: Click the **WLAN ID** of the SSID created in Procedure 2. (Example: WLAN-Data)



Step 3: On the General tab, in the Interface/Interface Group(G) list, choose the interface created in Procedure 8, and then click **Apply**. (Example: wireless-data)

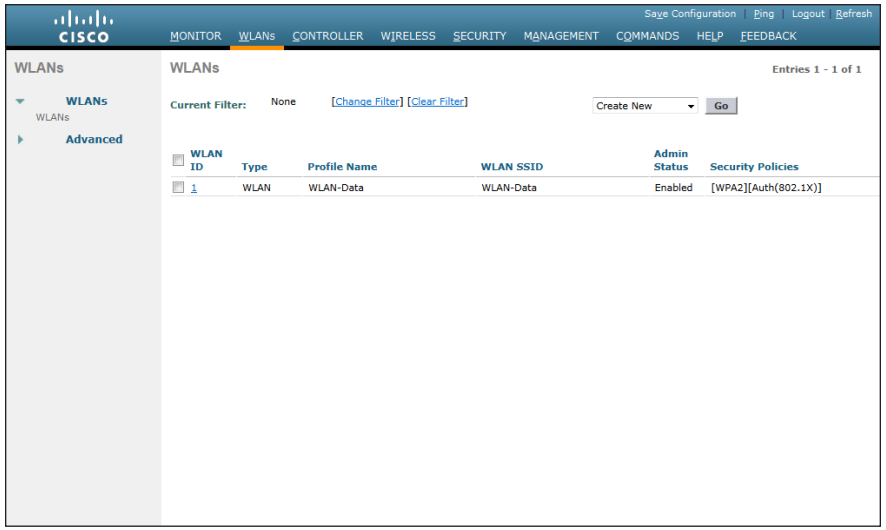


Procedure 11 Configure the voice wireless LAN

Wireless voice traffic is different from data traffic in that it cannot effectively handle delay and jitter as well as packet loss. To configure the voice WLAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

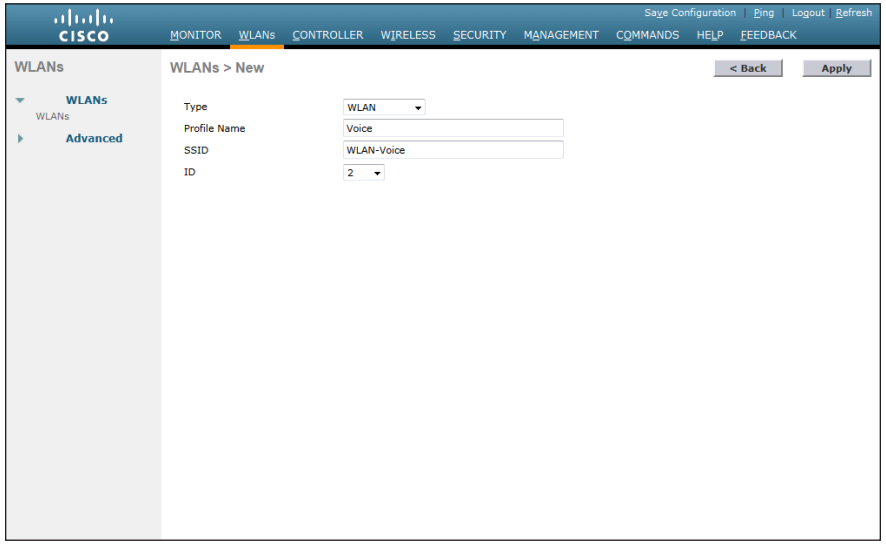
Step 1: Navigate to **WLANs**.

Step 2: In the drop-down list, choose **Create New**, and then click **Go**.



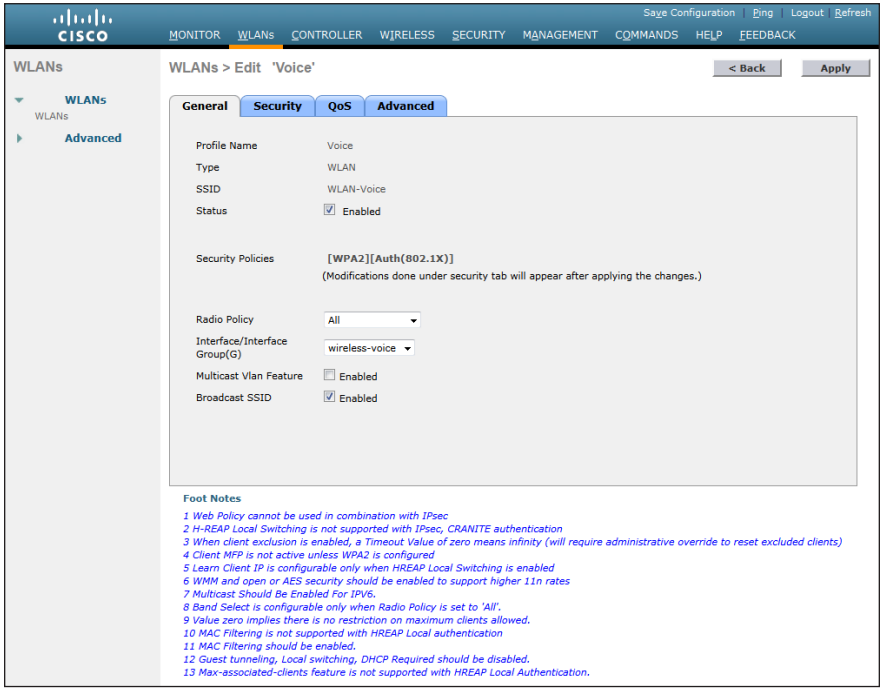
Step 3: Enter the **Profile Name**. (Example: Voice)

Step 4: In the SSID box, enter the voice WLAN name, and then click **Apply** (Example: WLAN-Voice)

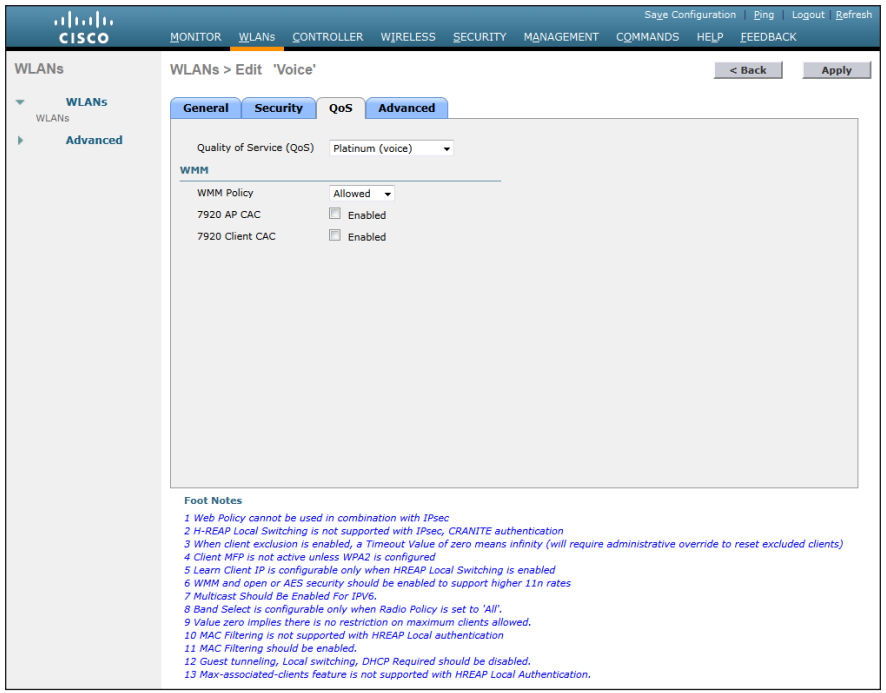


Step 5: On the General tab, next to Status, select **Enabled**.

Step 6: In the Interface/Interface Group(G) list, choose the interface created in Procedure 9. (Example: wireless-voice)



Step 7: On the QoS tab, in the Quality of Service (QoS) list, choose **Platinum (voice)**, and then click **Apply**.



Procedure 12 Configure the resilient controller

Although a standalone controller can support lightweight access points across multiple floors and buildings simultaneously, you should deploying multiple controllers at a site for resiliency.

This design uses two controllers. The first is the primary controller, which access points normally register to. The secondary controller, also called the *resilient controller*, provides resiliency in case the primary controller fails. Under normal operation, no access points will register to the resilient controller.

Even when configured as a pair, controllers do not share configuration information, so you must configure each controller separately.

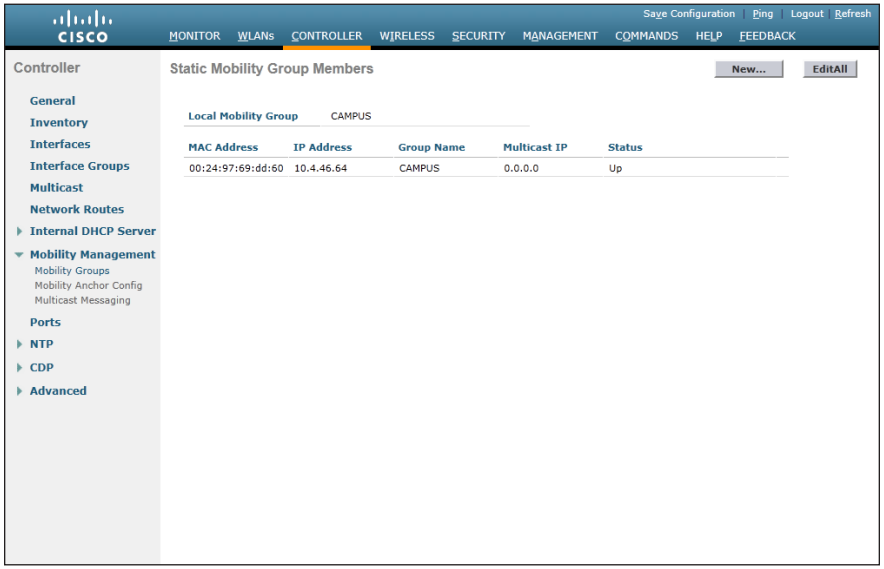
Step 1: Repeat Procedure 2 through Procedure 11 for the resilient controller.

Procedure 13 Configure mobility groups

Because it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be deployed in the same mobility group.

A *mobility group* is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when intercontroller or intersubnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices. With this information, the network can support intercontroller WLAN roaming and controller redundancy.

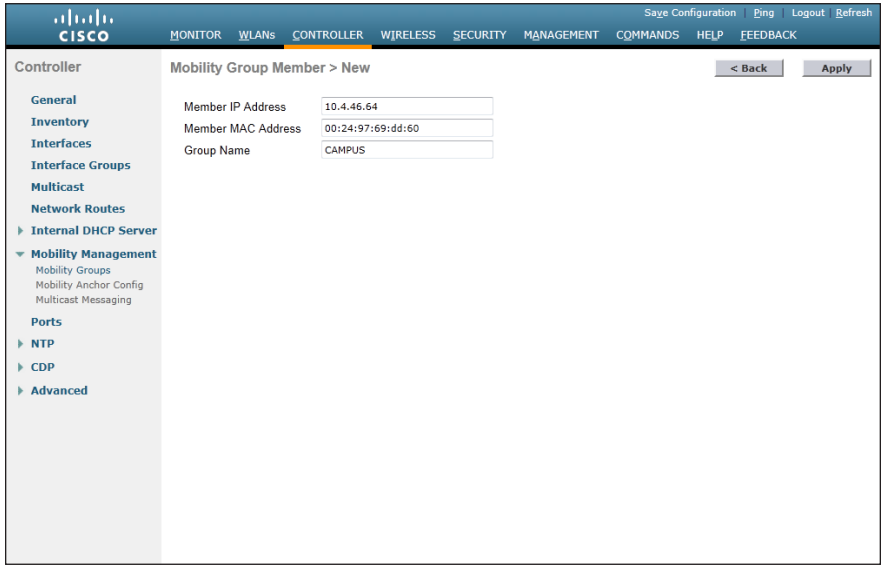
Step 1: On the primary controller, navigate to **Controller** > **Mobility Management** > **Mobility Groups**. The MAC address, IP address, and mobility group name for the local controller is shown.



Step 2: On the resilient controller, navigate to **Controller** > **Mobility Management** > **Mobility Groups**, and then click **New**.

Step 3: In the **Member IP Address** box, enter the IP address of the primary controller. (Example: 10.4.46.64)

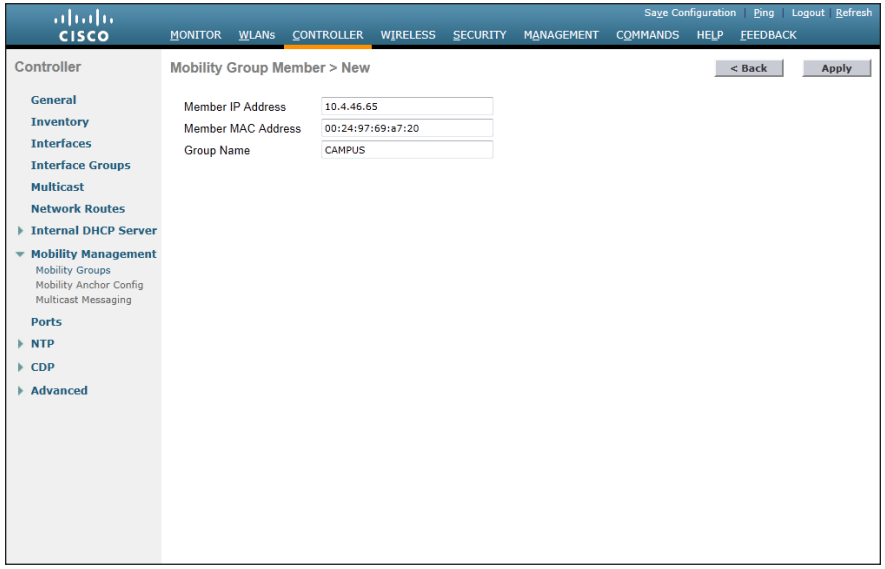
Step 4: In the **Member MAC Address** box, enter the MAC address of the primary controller, and then click **Apply**.



Step 5: On the primary controller, navigate to **Controller** > **Mobility Management** > **Mobility Groups**, and then click **New**.

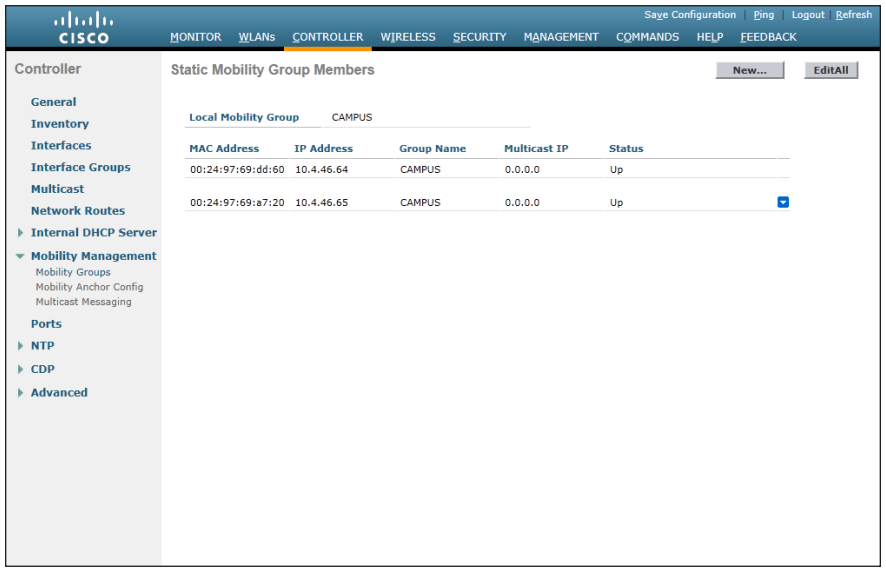
Step 6: In the **Member IP Address** box, enter the IP address of the resilient controller. (Example: 10.4.46.65)

Step 7: In the **Member MAC Address** box, enter the MAC address of the resilient controller, and then click **Apply**.



Step 8: On each controller, click **Save Configuration**, and then click **OK**.

Step 9: Navigate to Controller > Mobility Management > Mobility Groups, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as Up.



Procedure 14 Configure controller discovery

You have three options to configure controller discovery, depending on the number of controllers and the type of DHCP server you've deployed.

If you have only one controller pair in your organization, perform the steps in Option 1 of this procedure.

If you have deployed multiple controllers in your organization, use Dynamic Host Control Protocol (DHCP) Option 43 to map access points to their controllers. Using Option 43 allows remote sites, and each campus to define a unique mapping. Perform the steps in Option 2 or Option 3 of this procedure, depending on the type of DHCP server deployed in your organization.

Option 1. Only one WLC pair in the organization

Step 1: Configure the organization's DNS servers (in this case, 10.4.48.10) to resolve the **cisco-capwap-controller** host name to the management IP address of the controller (in this case, 10.4.46.64). The cisco-capwap-controller DNS record provides bootstrap information for access points that run software version 6.0 and higher.

Step 2: If the network may include access points that run software older than version 6.0, add a DNS record to resolve the host name cisco-lwapp-controller to the management IP address of the controller.

Option 2. Multiple WLC pairs in the organization: Cisco IOS DHCP server

In a network where there is no external, central-site DHCP server, you can provide DHCP service in Cisco IOS Software. This function can also be useful at a remote site where you want to provide local DHCP service and not depend on the WAN link to an external, central-site DHCP server.

Step 1: Assemble the DHCP option 43 value.

The hexadecimal string is assembled as a sequence of the Type + Length + Value (TLV) values for the Option 43 suboption.

- *Type* is always the suboption code 0xf1.
- *Length* is the number of controller management IP addresses times 4, in hexadecimal.
- *Value* is the IP address of the controller listed sequentially, in hexadecimal.

For example, suppose there are two controllers with management interface IP addresses 10.4.46.64 and 10.4.46.65. The type is 0xf1. The length is 2 * 4 = 8 = 0x08. The IP addresses translate to 0a042e40 (10.4.46.64) and 0a042e41(10.4.46.65). When the string is assembled, it yields **f1080a042e400a042e41**.

Step 2: On the network device, add option 43 to the pre-existing data network DHCP Pool.

```
ip dhcp pool [pool name]
 option 43 hex f1080a042e400a042e41
```

Option 3. Multiple WLC pairs: Microsoft DHCP Server

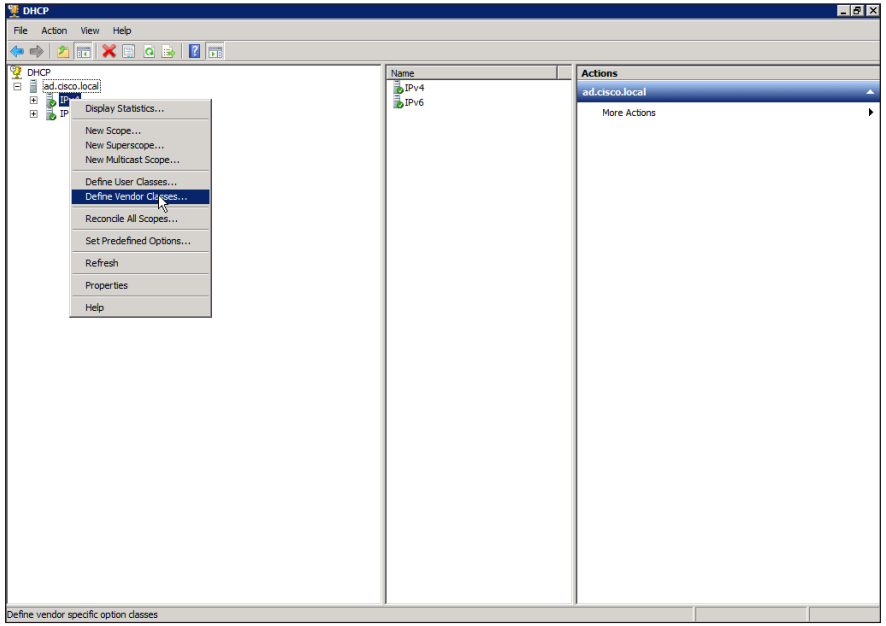
This procedure shows how the Windows DHCP server is configured in order to return vendor-specific information to the lightweight Cisco Aironet 1040 and 2600 Series Access Points used in this deployment guide. The vendor class identifier for a lightweight Cisco Aironet series access point is specific to each model type. To support more than one access point model, you must create a vendor class for each model type.

Table 3 - Vendor class identifiers

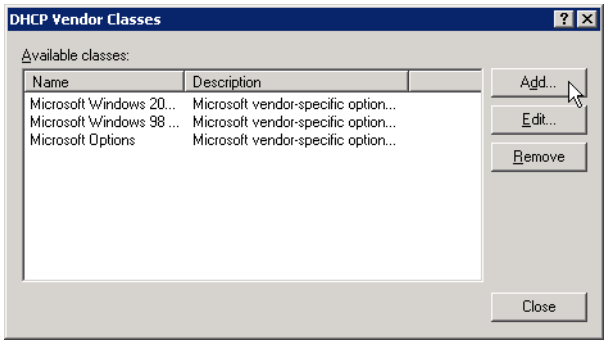
Access point	Vendor class identifier
Cisco Aironet 1040 Series	Cisco AP c1040
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600

Step 1: Open the DHCP Server Administration Tool or MMC.

Step 2: Right-click the **DHCP root,> IPv4**, and then click **Define Vendor Classes**.



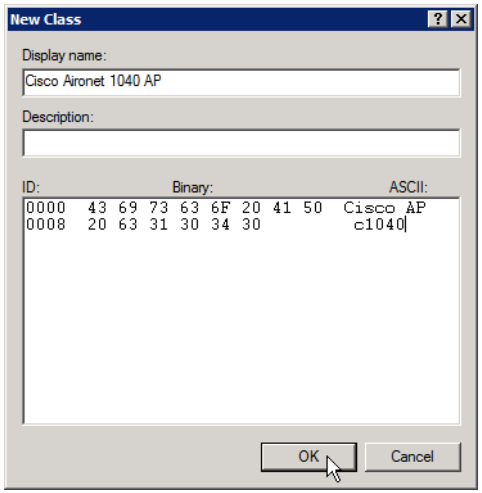
Step 3: In the DHCP Vendor Classes window, click **Add**.



Step 4: In the New Class dialog box, enter a **Display Name**. (Example: Cisco Aironet 1040 AP)

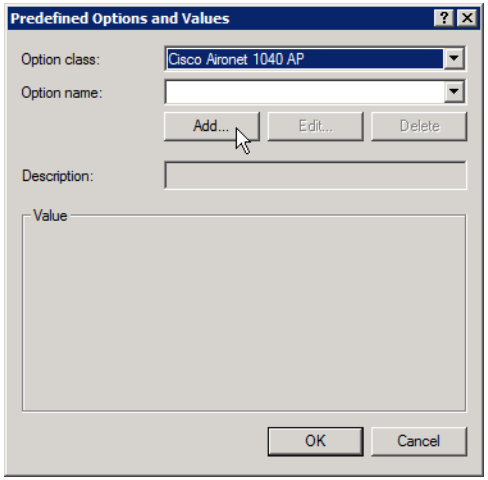
Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 3, and then click **OK**. (Example: Cisco AP c1040)

Step 6: In the DHCP Vendor Classes window, click **Close**.



Step 7: Right-click the **DHCP Server Root**, and then choose **Set Predefined Options**.

Step 8: In the Option Class list, choose the class created in Step 4, and then click **Add**.

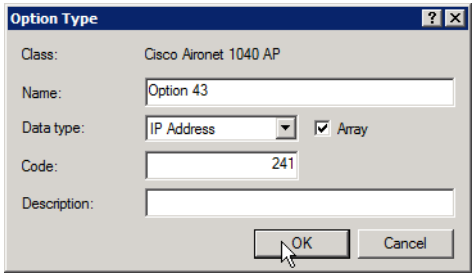


Step 9: In the Option Type dialog box, enter a **Name**. (Example: Option 43)

Step 10: In the Data Type list, choose **IP Address**.

Step 11: Select **Array**.

Step 12: In the **Code** box, enter **241**, and then click **OK**.



The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

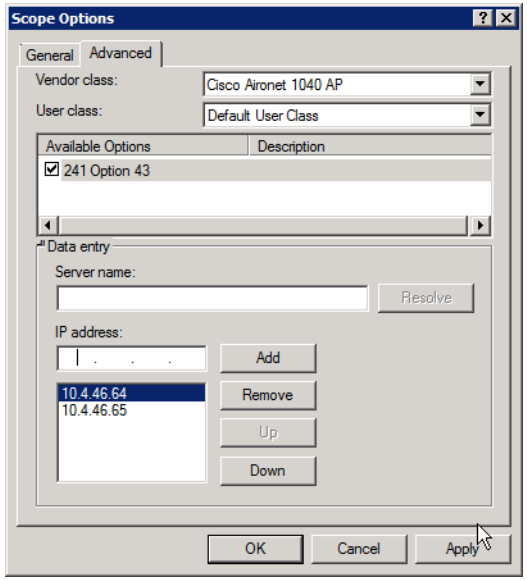
Step 13: Choose the appropriate DHCP scope, right-click **Scope Options**, and then choose **Configure Options**.

Step 14: Click the **Advanced** tab, and in the Vendor class list, choose the class created in Step 4.

Step 15: Under Available Options, select **241 Option 43**.

Step 16: In the **IP address** box, enter the IP address of the primary controller's management interface, and then click **Add**. (Example: 10.4.46.64)

Step 17: Repeat Step 16 for the resilient controller, and then click **Apply**. (Example: 10.4.46.65)



Procedure 15 Connect the access points

On the LAN access switch, the switch interfaces that are connected to the access points use the standard access switchport configuration, with the exception of the QoS policy that you configure in this procedure.

Step 1: Configure the interface where the access point will be connected to trust the QoS marking from the access point.

```
interface GigabitEthernet [port]
  description Access Point Connection
  switchport access vlan 100
  switchport voice vlan 101
  switchport host
  macro apply EgressQoS
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security aging type inactivity
  switchport port-security violation restrict
  ip arp inspection limit rate 100
  ip dhcp snooping limit rate 100
  ip verify source
```

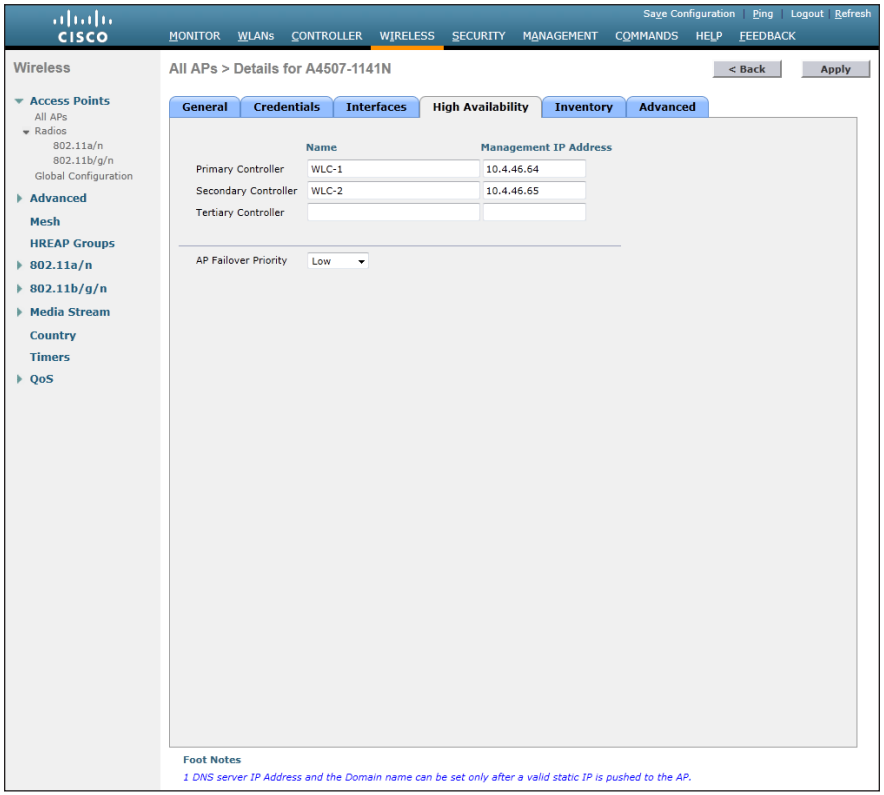
Procedure 16 Configure access points for resiliency

Step 1: On the primary controller, navigate to **Wireless** and select the desired access point.

Step 2: Click the **High Availability** tab.

Step 3: In the **Primary Controller** box, enter the name and management IP address of the primary controller. (Example: WLC-1 / 10.4.46.64)

Step 4: In the **Secondary Controller** box, enter the name and management IP address of the resilient controller and then click **Apply.** (Example: WLC-2 / 10.4.46.65)



Process

Configuring Remote-Site Wireless with FlexConnect

1. Configure the LAN distribution switch
2. Configure the WLC platform
3. Configure the time zone
4. Configure SNMP
5. Limit what networks can manage the WLC
6. Configure wireless user authentication
7. Configure management authentication
8. Configure the resilient WLC
9. Configure mobility groups
10. Configure the data wireless LAN
11. Configure the voice wireless LAN
12. Configure controller discovery
13. Configure the remote-site router
14. Configure the remote-site switch for APs
15. Configure the AP for Cisco FlexConnect
16. Configure access points for resiliency
17. Configure FlexConnect Groups

There are two methods of deploying remote site wireless LAN controllers: shared and dedicated.

- A shared WLC has both remote-site access points and local, on-site access points connected to it concurrently. Use a shared WLC when the number of access points matches the available capacity of the co-located WLCs near the WAN headend, and the WAN headend is co-located with a campus.
- A dedicated WLC only has remote-site access points connected to it. Use a dedicated WLC when you have a large number of access points or remote sites. You also use this option when the co-located WLCs near the WAN headend don't have the necessary capacity or the WAN headend is not co-located with a campus.

If you are using a shared WLC, this deployment guide assumes that you have already deployed the WLC following the instructions in the Configuring Wireless Using On-Site Controllers process. To deploy remote-site wireless in a shared controller deployment, skip to Procedure 10.

If you are using a dedicated WLC, perform all the procedures in this process to deploy remote-site wireless.

Table 4 - Cisco remote site wireless controller parameters checklist

Parameter	Cisco SBA values primary controller	Cisco SBA values resilient controller	Site-specific values
Controller parameters (optional)			
Switch Interface Number	1/0/3, 2/0/3	1/0/4, 2/0/4	
VLAN number	146		
Time zone	PST -8 0		
IP address	10.4.46.68/24	10.4.46.69/24	
Default gateway	10.4.46.1		
Hostname	WLC-RemoteSites-1	WLC-RemoteSites-2	
Mobility group name	REMOTES		
RADIUS server IP address	10.4.48.15		
RADIUS shared key	SecretKey		
Management network (optional)	10.4.48.0/24		
TACACS server IP address (optional)	10.4.48.15		
TACACS shared key (optional)	SecretKey		
Remote site parameters			
Wireless data SSID	WLAN-Data		
Wireless data VLAN number	65		
Wireless voice SSID	WLAN-Voice		
Wireless voice VLAN number	70		
Default gateway	10.4.20.1		
Controller interface IP address	10.4.20.5/22	10.4.20.6/22	

Procedure 1 Configure the LAN distribution switch

Step 1: On the LAN distribution switch, create the wireless management VLAN that you are connecting to the distribution switch.

```
vlan 146
 name WLAN_Mgmt
```

Step 2: Configure a VLAN interface (SVI) for the VLAN so devices in the VLAN can communicate with the rest of the network.

```
interface Vlan146
 description Wireless Management Network
 ip address 10.4.46.1 255.255.255.0
 no shutdown
```

Step 3: For interface configuration, an 802.1Q trunk is used for the connection to the WLCs. This allows the distribution switch to provide the Layer 3 services to all of the networks defined on the WLC. The VLANs allowed on the trunk are reduced to only the VLANs that are active on the WLC.

If you are deploying the Catalyst 4500 LAN distribution switch, you do not need to use the **switchport trunk encapsulation dot1q** command in the following configurations.

If you are deploying a Cisco 7500 Series Wireless LAN Controller, configure a 10 Gigabit distribution switch interface as a trunk. Note that when deploying a Cisco 7500 Series Wireless LAN Controller, the WLC should not be connected to a 3750X distribution switch.

```
interface TenGigabitEthernet [number]
 description To WLC port 1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 146
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

If you are deploying a Cisco 5500 Series Wireless LAN Controller, configure at least two distribution switch interfaces as an EtherChannel trunk.

```
interface GigabitEthernet [port 1]
 description To WLC Port 1
interface GigabitEthernet [port 2]
 description To WLC Port 2
!
interface range GigabitEthernet [port 1], GigabitEthernet
[port 2]
  switchport
  macro apply EgressQoS
  channel-group [number] mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
!
interface Port-channel [number]
 description To WLC
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 146
 switchport mode trunk
 logging event link-status
 no shutdown
```

Procedure 2 Configure the WLC platform

After the WLC is physically installed and powered up, you will see the following on the console:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: YES
```

Step 1: Enter a system name. (Example: WLC-RemoteSites-1)

```
System Name [Cisco_d9:3d:66] (31 characters max): WLC-
RemoteSites-1
```

Step 2: Enter an administrator username and password.

Tech Tip

Use at least three of the following four classes in the password: lowercase letters, uppercase letters, digits or special characters.

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****
```

Step 3: Use DHCP for the service port interface address.

```
Service Interface IP address Configuration [none] [DHCP]: DHCP
```

Step 4: Enter the IP address and subnet mask for the management interface.

If you are deploying a Cisco 7500 Series Wireless LAN Controller, configure the 10 Gigabit interface as a trunk.

```
Management Interface IP Address: 10.4.46.68
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.46.1
Management Interface VLAN Identifier (0 = untagged): 146
Management Interface Port Num [1 to 2]: 1
```

If you are deploying a Cisco 5500 Series Wireless LAN Controller, configure at least two interfaces as an EtherChannel trunk.

```
Enable Link Aggregation (LAG) [yes][NO]: YES
Management Interface IP Address: 10.4.46.68
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.46.1
Management Interface VLAN Identifier (0 = untagged): 146
```

Step 5: Enter the default DHCP server for clients. (Example: 10.4.48.10)

```
Management Interface DHCP Server IP Address: 10.4.48.10
```

Step 6: The virtual interface is used by the WLC for Mobility DHCP relay and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

```
Virtual Gateway IP Address: 192.0.2.1
```

Step 7: Enter a name that will be used as the default mobility and RF group. (Example: REMOTES)

```
Mobility/RF Group Name: REMOTES
```

Step 8: Enter an SSID for the WLAN that supports data traffic. You will be able to leverage this later in the deployment process.

```
Network Name (SSID): WLAN-Data
Configure DHCP Bridging Mode [yes][NO]: NO
```

Step 9: For increased security, enable DHCP snooping.

```
Allow Static IP Addresses {YES][no]: NO
```

Step 10: You will configure the RADIUS server later by using the GUI.

```
Configure a RADIUS Server now? [YES][no]: NO
```

Step 11: Enter the correct country code for the country where you are deploying the WLC.

```
Enter Country Code list (enter 'help' for a list of countries)
[US]: US
```

Step 12: Enable all wireless networks.

```
Enable 802.11b network [YES][no]: YES
Enable 802.11a network [YES][no]: YES
Enable 802.11g network [YES][no]: YES
```

Step 13: Enable the RRM auto-RF feature. This helps you keep your network up and operational.

```
Enable Auto-RF [YES][no]: YES
```

Step 14: Synchronize the WLC clock to your organization's NTP server.

```
Configure a NTP server now? [YES][no]:YES
Enter the NTP server's IP address: 10.4.48.17
Enter a polling interval between 3600 and 604800 secs: 86400
```

Step 15: Save the configuration. If you respond with **no**, the system will restart without saving the configuration and you will have to complete this procedure again.

```
Configuration correct? If yes, system will save it and reset.
[yes][NO]: YES
Configuration saved!
Resetting system with new configuration
```

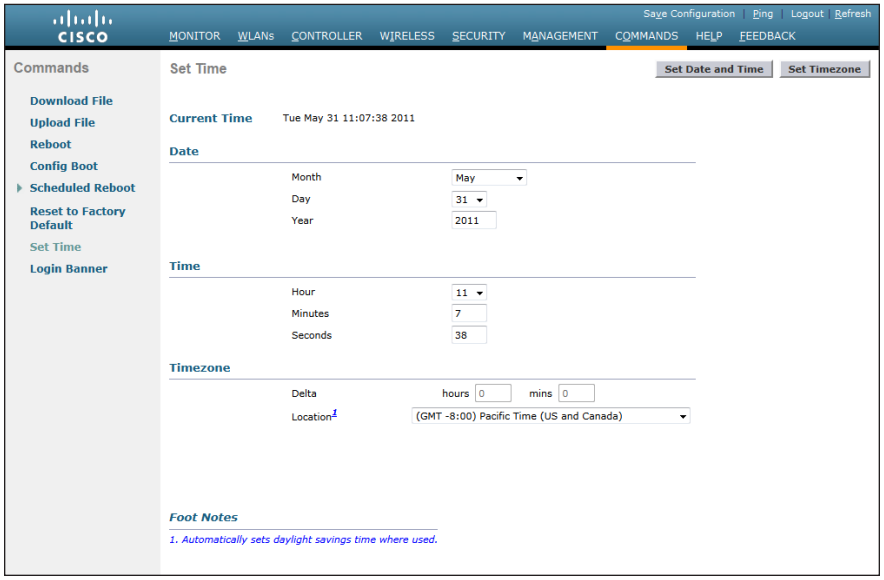
Step 16: After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page using the credentials defined in Step 2. (Example: https://WLC-RemoteSites-1.cisco.local/)

Procedure 3 Configure the time zone

Step 1: Navigate to **Commands > Set Time.**

Step 2: In the Location list, choose the time zone that corresponds to the location of the WLC.

Step 3: Click **Set Timezone**.



Procedure 4 Configure SNMP

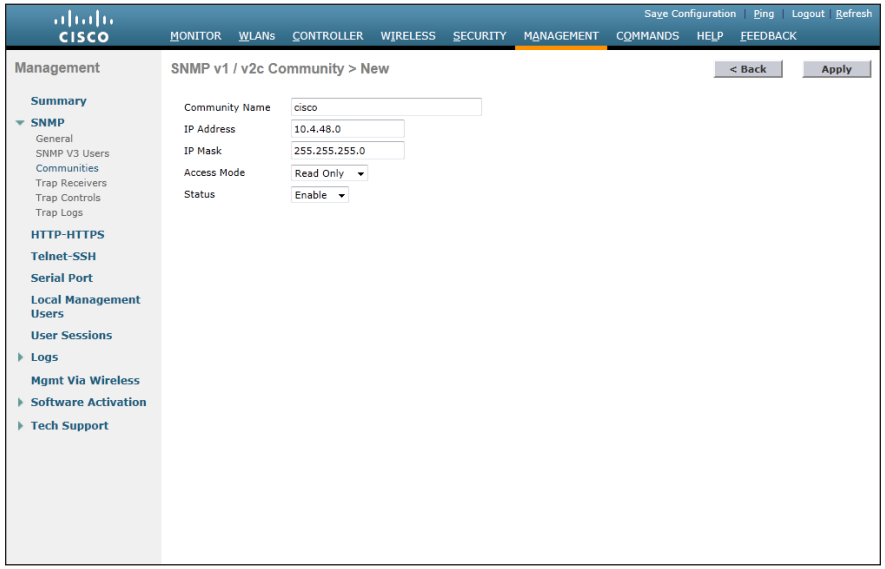
Step 1: In **Management** > **SNMP** > **Communities**, click **New**.

Step 2: Enter the **Community Name**. (Example: cisco)

Step 3: Enter the **IP Address.** (Example: 10.4.48.0)

Step 4: Enter the **IP Mask**. (Example: 255.255.255.0)

Step 5: In the Status list, choose **Enable**, and then click **Apply**.



Step 6: In **Management** > **SNMP** > **Communities**, click **New**.

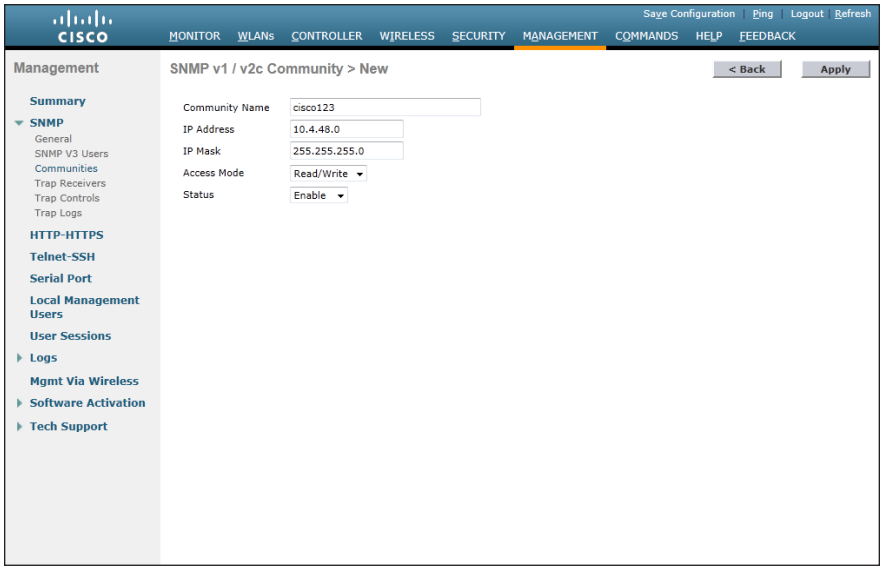
Step 7: Enter the **Community Name**. (Example: cisco123)

Step 8: Enter the **IP Address.** (Example: 10.4.48.0)

Step 9: Enter the **IP Mask**. (Example: 255.255.255.0)

Step 10: In the Access Mode list, choose **Read/Write**.

Step 11: In the Status list, choose **Enable** and then click **Apply.**

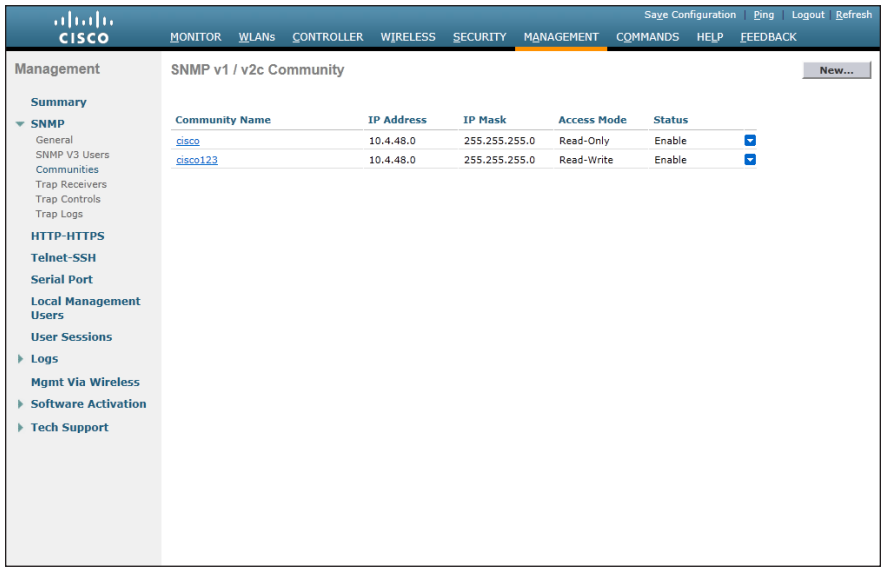


Step 12: Navigate to **Management** > **SNMP** > **Communities**.

Step 13: Point to the blue box for the **public** community, and then click **Remove**.

Step 14: On the message "Are you sure you want to delete?", click **OK**.

Step 15: Repeat Step 13 and Step 14 for the private community.



Procedure 5 Limit what networks can manage the WLC

(Optional)

In networks where network operational support is centralized you can increase network security by using an access list to limit the networks that can access your controller. In this example, only devices on the 10.4.48.0/24 network will be able to access the controller via SSH or SNMP.

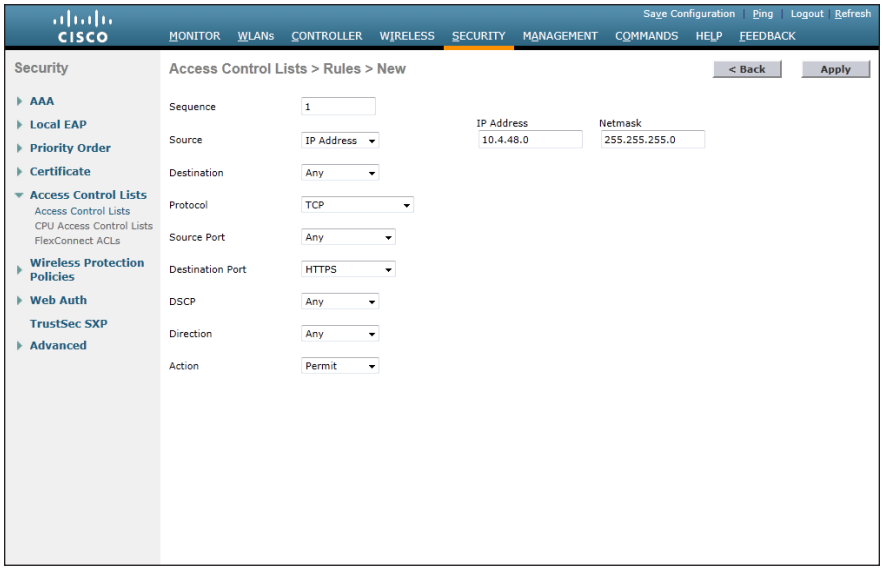
Step 1: In **Security** > **Access Control Lists** > **Access Control Lists**, click **New**.

Step 2: Enter an Access Control List Name, and then click **Apply**.

Step 3: In the list, choose the name of the access list you just created, and then click **Add New Rule**.

Step 4: In the window, enter the following configuration details, and then click **Apply**.

- Sequence — 1
- Source — 10.4.48.0 / 255.255.255.0
- Destination — Any
- Protocol — TCP
- Destination Port — HTTPS
- Action — Permit



Step 5: Repeat Step 1 through Step 4 four more times, using the configuration details in the following table.

Sequence	Source	Destination	Protocol	Destination Port	Action
2	10.4.48.0/ 255.255.255.0	Any	TCP	Other/22	Permit
3	Any	Any	TCP	HTTPS	Deny
4	Any	Any	TCP	Other/22	Deny
5	Any	Any	Any	Any	Permit

Step 6: In **Security > Access Control Lists > CPU Access Control Lists**, select **Enable CPU ACL**.

Step 7: In the **ACL Name** list, choose the ACL you just created, and then click **Apply.**

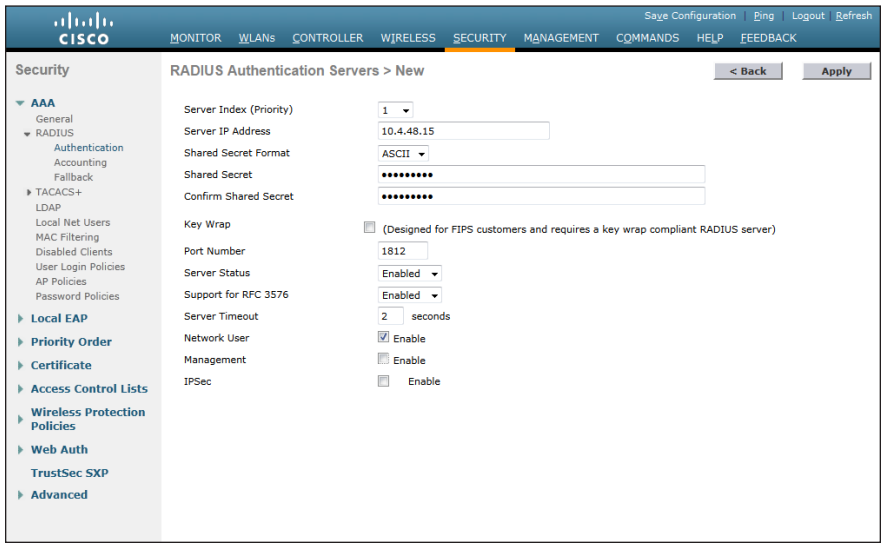
Procedure 6 Configure wireless user authentication

Step 1: In **Security > AAA > Radius > Authentication**, click **New**.

Step 2: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 3: Enter and confirm the **Shared Secret**. (Example: SecretKey)

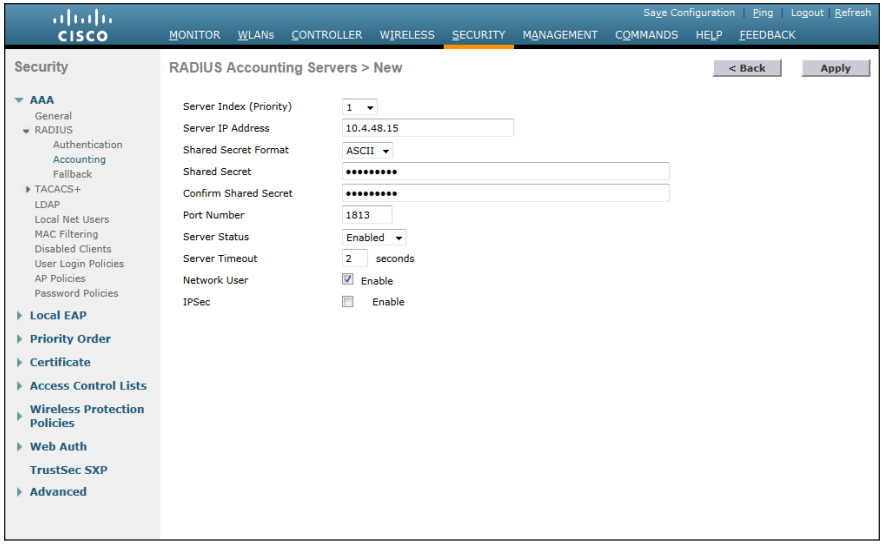
Step 4: To the right of Management , clear **Enable**, and then click **Apply**.



Step 5: In **Security > AAA > Radius > Accounting**, click **New**.

Step 6: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 7: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



Procedure 7 Configure management authentication

(Optional)

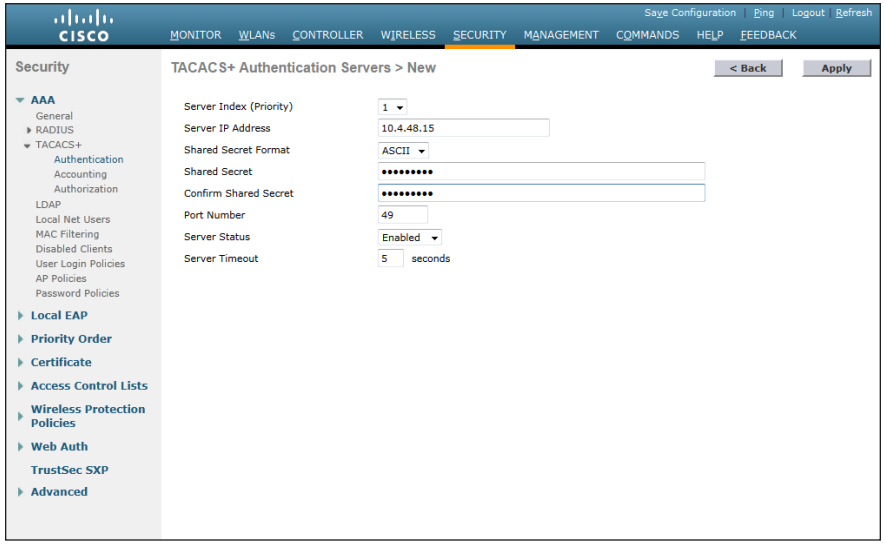
You can use this procedure to deploy centralized management authentication by configuring the Authentication, Authorization and Accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 8.

As networks scale in the number of devices to maintain, the operational burden to maintain local management accounts on every device also scales. A centralized Authentication, Authorization and Accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

Step 1: In **Security > AAA > TACACS+ > Authentication**, click **New**.

Step 2: Enter the **Server IP Address**. (Example: 10.4.48.15)

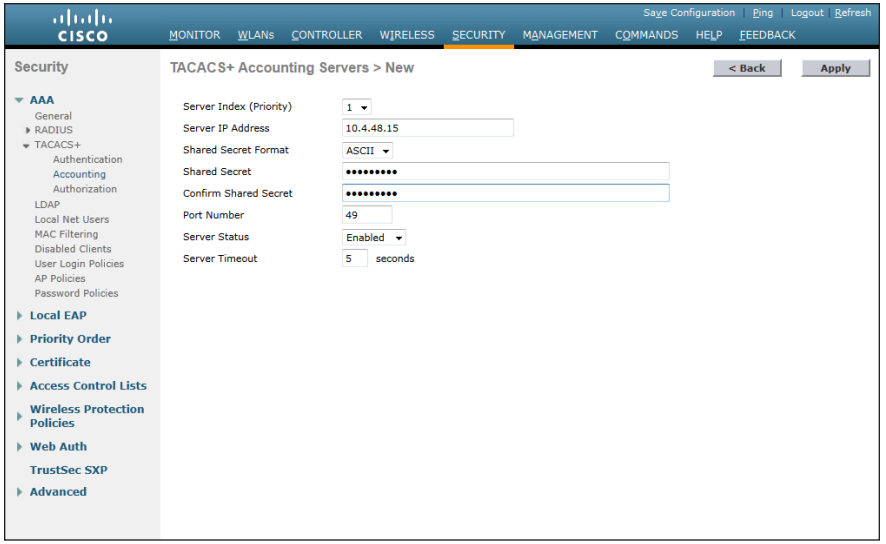
Step 3: Enter and confirm the **Shared Secret** ,and then click **Apply**. (Example: SecretKey)



Step 4: In **Security** > **AAA** > **TACACS+** > **Accounting**, click **New**.

Step 5: Enter the **Server IP Address**. (Example: 10.4.48.15)

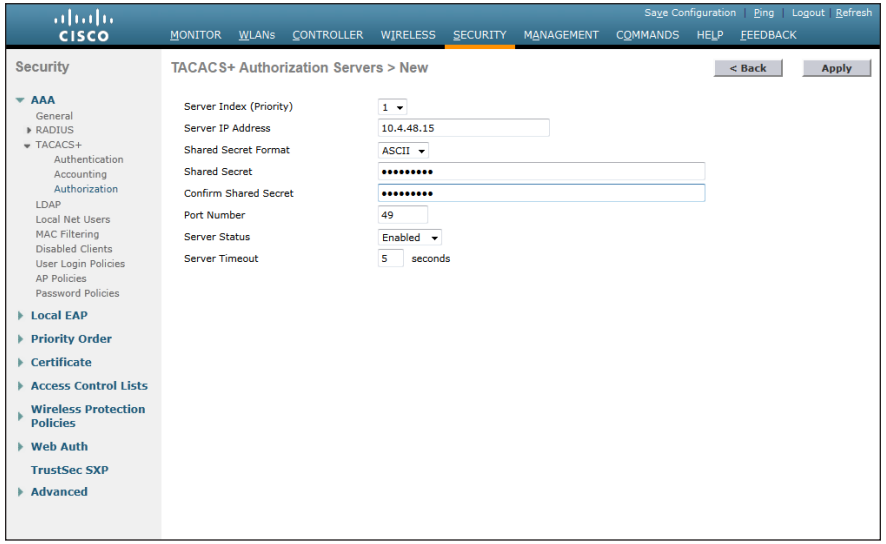
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



Step 7: In **Security** > **AAA** > **TACACS+** > **Authorization**, click **New**.

Step 8: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 9: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

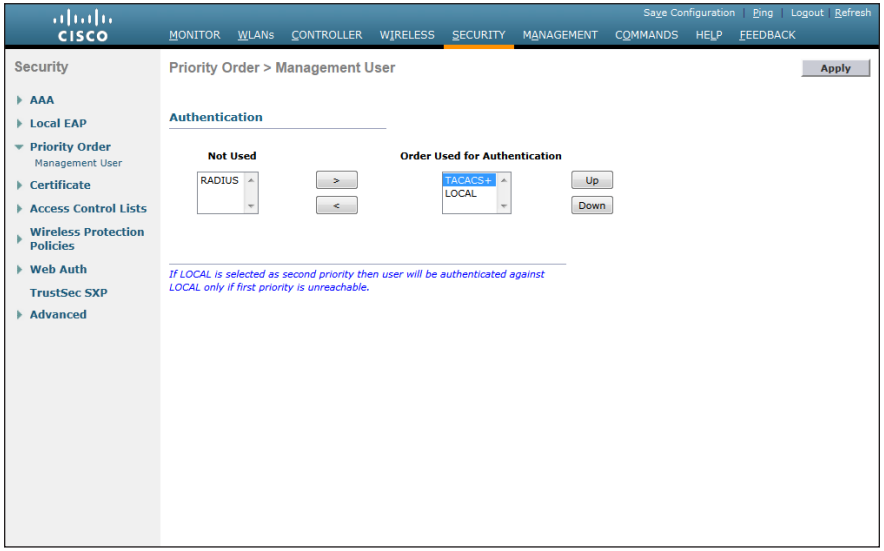


Step 10: Navigate to **Security** > **Priority Order** > **Management User**.

Step 11: Using the arrow buttons, move TACACS+ from the **Not Used** list to the **Used for Authentication** list.

Step 12: Using the **Up** and **Down** buttons, move TACACS+ to be the first in the **Order Used for Authentication** list.

Step 13: Using the arrow buttons, move RADIUS to the **Not Used** list, and then click **Apply**.



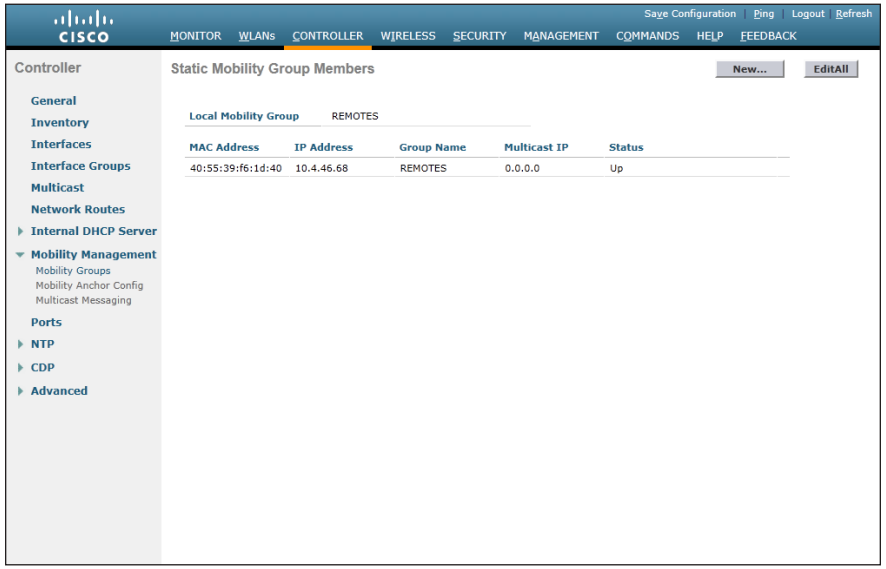
Procedure 8 Configure the resilient WLC

This design uses two WLCs. The first is the primary WLC, and the access points register to it. The second WLC provides resiliency in case the primary WLC fails. Under normal operation, there will not be any access points registered to this WLC.

Repeat Procedure 1through Procedure 7 for the resilient WLC.

Procedure 9 Configure mobility groups

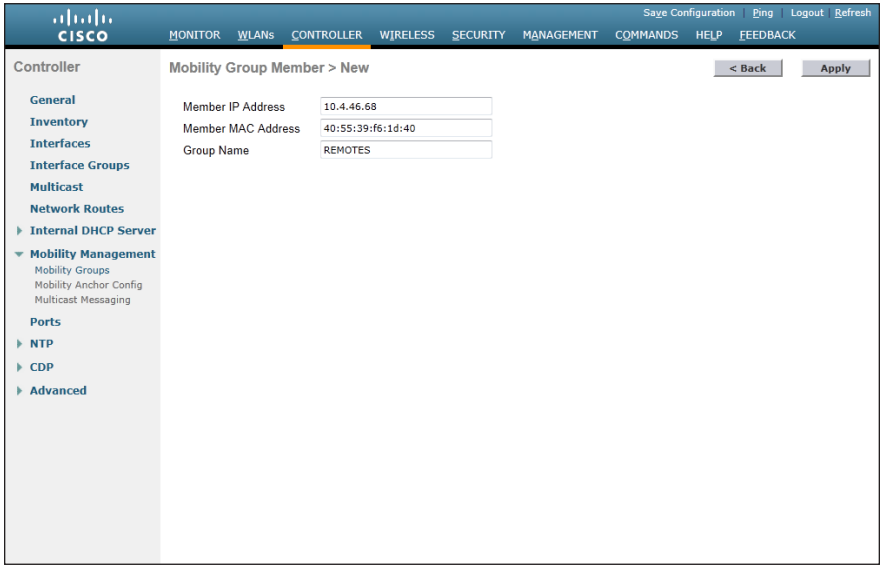
Step 1: On the primary controller, navigate to **Controller** > **Mobility Management** > **Mobility Groups**. The MAC address, IP address, and mobility group name for the local controller is shown on the Static Mobility Group Members page.



Step 2: On the resilient controller, navigate to **Controller** > **Mobility Management** > **Mobility Groups**, and then click **New**.

Step 3: In the **Member IP Address** box, enter the IP address of the primary controller. (Example: 10.4.46.68)

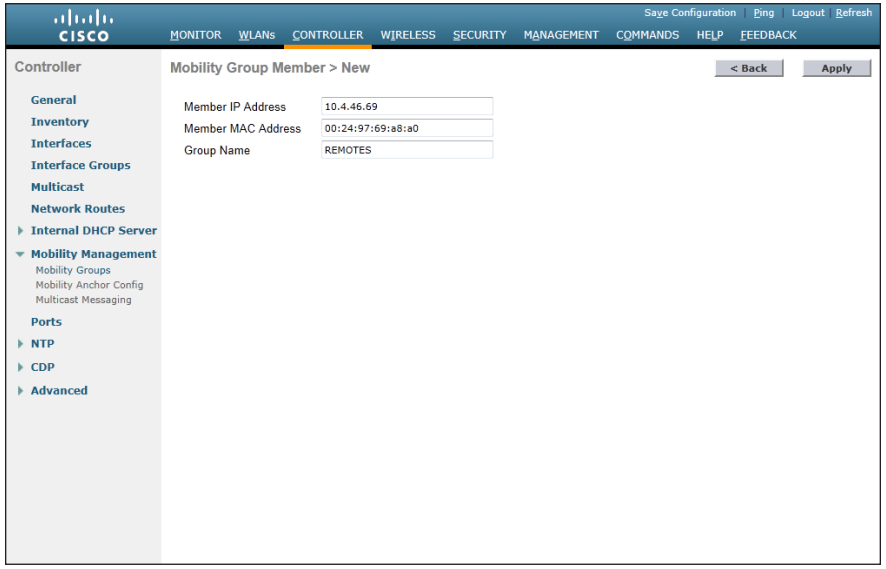
Step 4: In the **Member MAC Address** box, enter the MAC address of the primary controller, and then click **Apply**.



Step 5: On the primary controller, navigate to **Controller** > **Mobility Management** > **Mobility Groups**, and then click **New**.

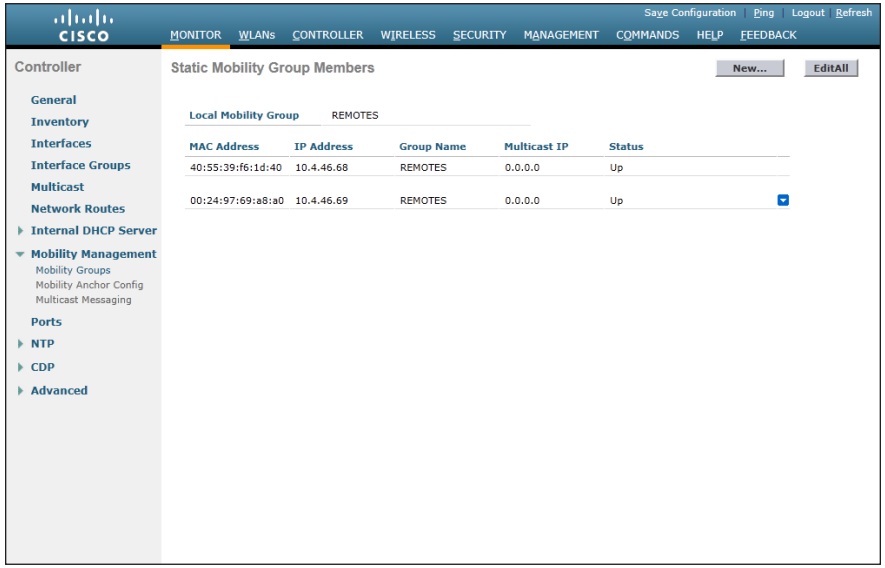
Step 6: In the **Member IP Address** box, enter the IP address of the resilient controller. (Example: 10.4.46.69)

Step 7: In the **Member MAC Address** box, enter the MAC address of the resilient controller, and then click **Apply**.



Step 8: On each controller, click **Save Configuration**, and then click **OK**.

Step 9: Navigate to **Controller** > **Mobility Management** > **Mobility Groups**, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as Up.

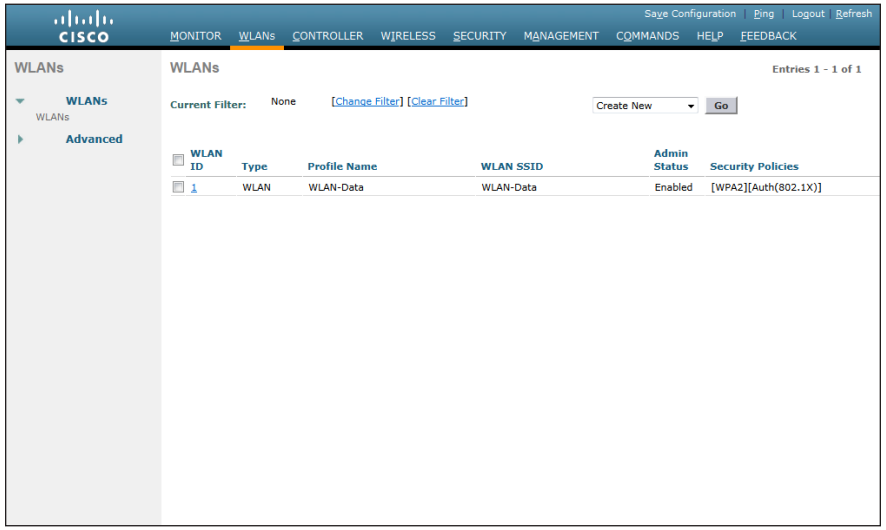


Procedure 10 Configure the data wireless LAN

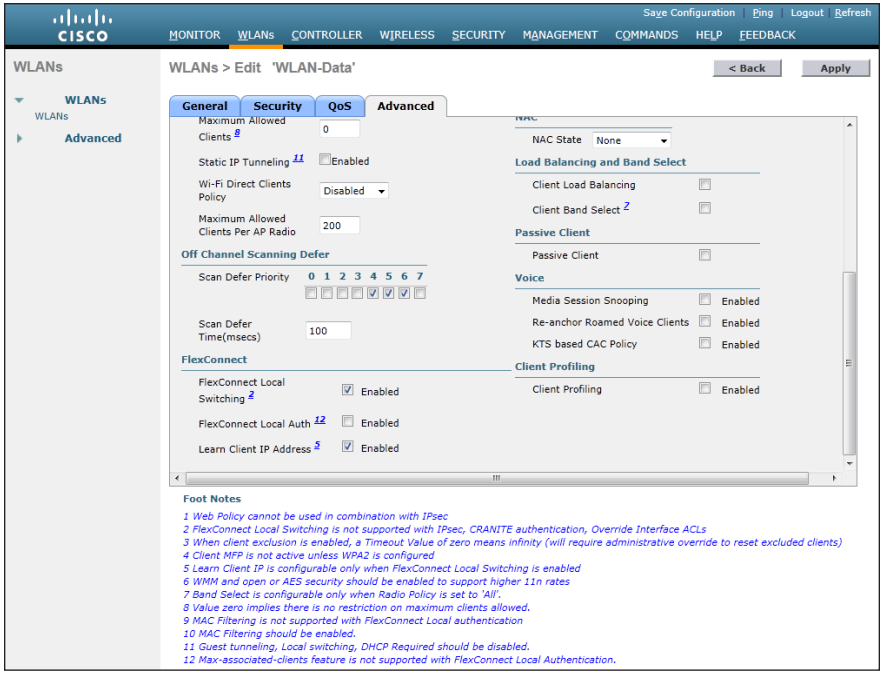
Wireless data traffic can handle delay, jitter, and packet loss more efficiently than wireless voice traffic.. For the data WLAN, keep the default QoS settings and segment the data traffic onto the data wired VLAN.

Step 1: Navigate to **WLANs**.

Step 2: Click the **WLAN ID** of the data SSID.



Step 3: On the Advanced tab, to the right of FlexConnect Local Switching, select **Enabled**, and then click **Apply**.

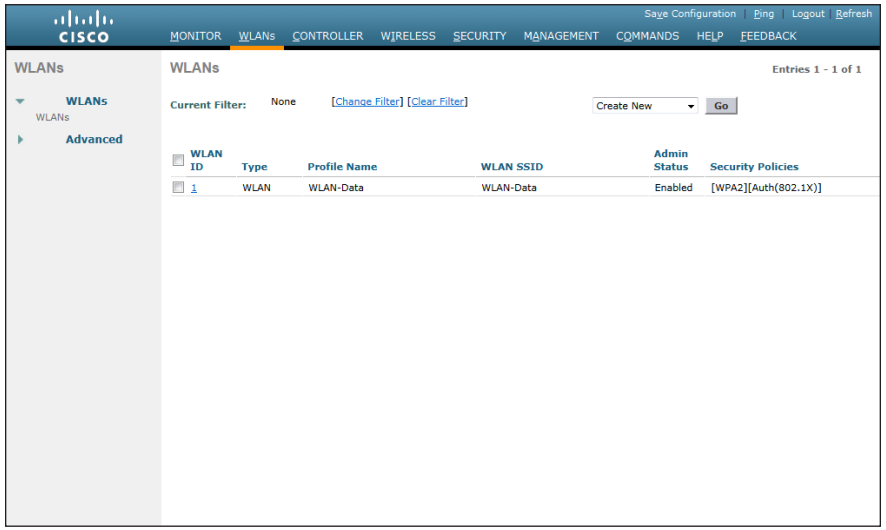


Procedure 11 Configure the voice wireless LAN

Wireless voice traffic is unique among other types of data traffic in that it cannot effectively handle delay and jitter or packet loss. To configure the voice WLAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

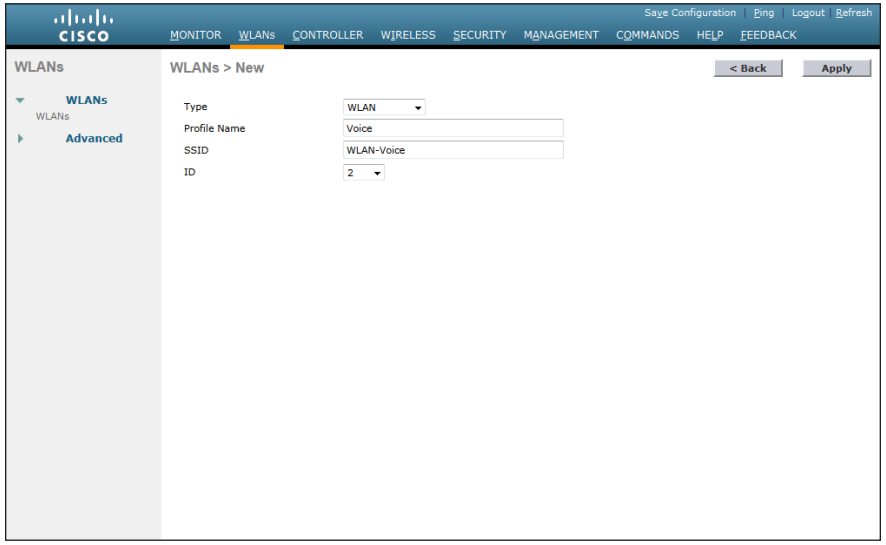
Step 1: Navigate to **WLANs**.

Step 2: In the drop-down list, choose **Create New**, and then click **Go**.

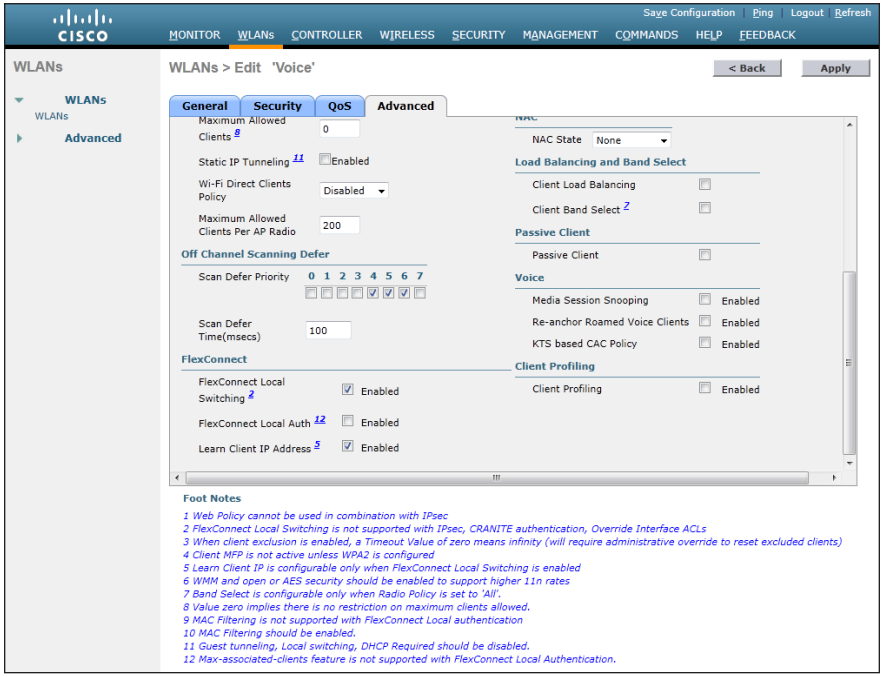


Step 3: Enter the **Profile Name**. (Example: Voice)

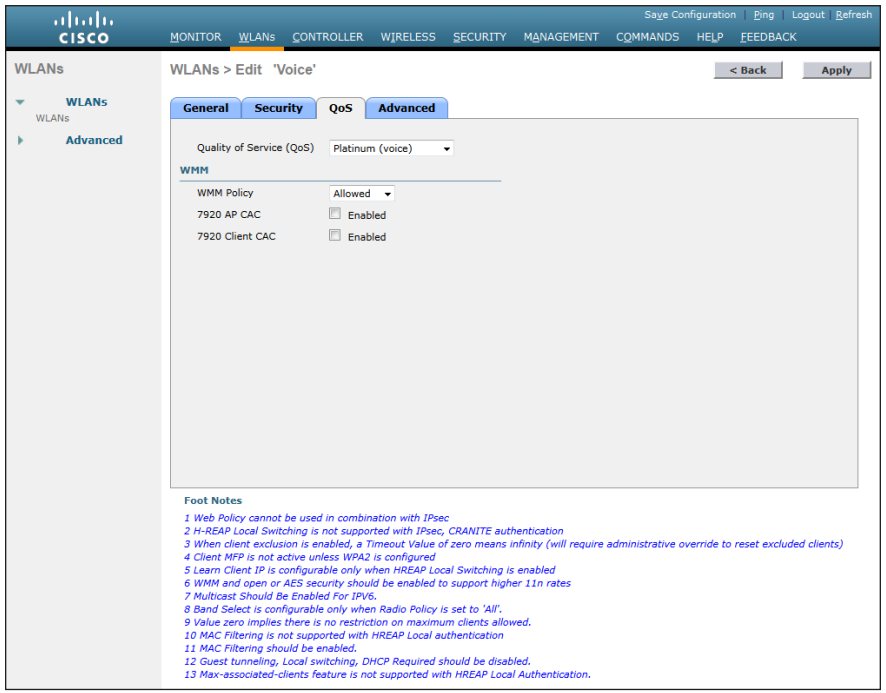
Step 4: In the **SSID** box, enter the voice WLAN name, and then click **Apply**. (Example: WLAN-Voice)



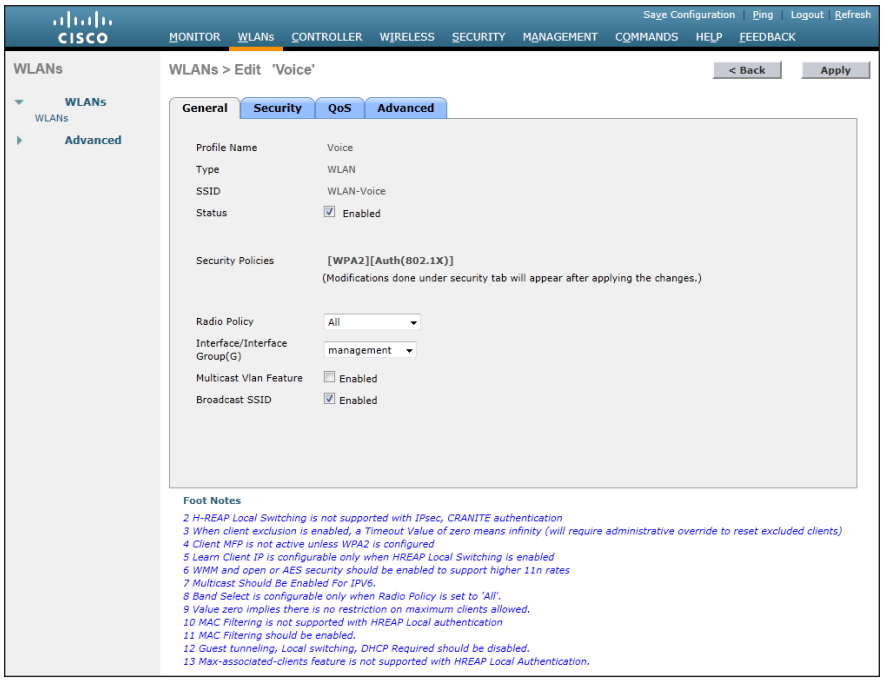
Step 5: On the Advanced tab, to the right of FlexConnect Local Switching, select **Enabled**, and then click **Apply**.



Step 6: On the QoS tab, in the Quality of Service (QoS) list, choose **Platinum (voice)**, and then click **Apply**.



Step 7: On the General tab, to the right of Status, select **Enabled**, and then click **Apply**.



Procedure 12 Configure controller discovery

You have three options to configure controller discovery, depending on the number of controllers and the type of DHCP server you've deployed.

If you have only one controller pair in your organization, perform the steps in Option 1 of this procedure.

If you have deployed multiple controllers in your organization, use Dynamic Host Control Protocol (DHCP) Option 43 to map access points to their controllers. Using Option 43 allows remote sites, and each campus to define a unique mapping. Perform the steps in Option 2 or Option 3 of this procedure, depending on the type of DHCP server deployed in your organization.

Option 1. Only one WLC pair in the organization

Step 1: Configure the organization's DNS servers (in this case, 10.4.48.10) to resolve the **cisco-capwap-controller** host name to the management IP address of the controller (in this case, 10.4.46.64). The cisco-capwap-controller DNS record provides bootstrap information for access points that run software version 6.0 and higher.

Step 2: If the network may include access points that run software older than version 6.0, add a DNS record to resolve the host name **cisco-lwapp-controller** to the management IP address of the controller.

Option 2. Multiple WLC pairs in the organization: Cisco IOS DHCP server

In a network where there is no external central site DHCP server you can provide DHCP service in Cisco IOS Software. This function can also be useful at a remote-site where you want to provide local DHCP service and not depend on the WAN link to an external central site DHCP server.

Step 1: Assemble the DHCP option 43 value.

The hexadecimal string is assembled as a sequence of the Type+Length+Value (TLV) values for the Option 43 suboption.

- *Type* is always the suboption code 0xf1.
- *Length* is the number of controller management IP addresses times 4 in hex.
- *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose there are two controllers with management interface IP addresses, 10.4.46.64 and 10.4.46.65. The type is 0xf1. The length is 2 * 4 = 8 = 0x08. The IP addresses translate to 0a042e44 (10.4.46.68) and 0a042e45(10.4.46.69). When the string is assembled, it yields **f1080a042e440a042e45**.

Step 2: On the network device, add option 43 to the pre-existing data network DHCP Pool.

```
ip dhcp pool [pool name]
 option 43 hex f1080a042e440a042e45
```

Option 3: Multiple WLC pairs: Microsoft DHCP Server

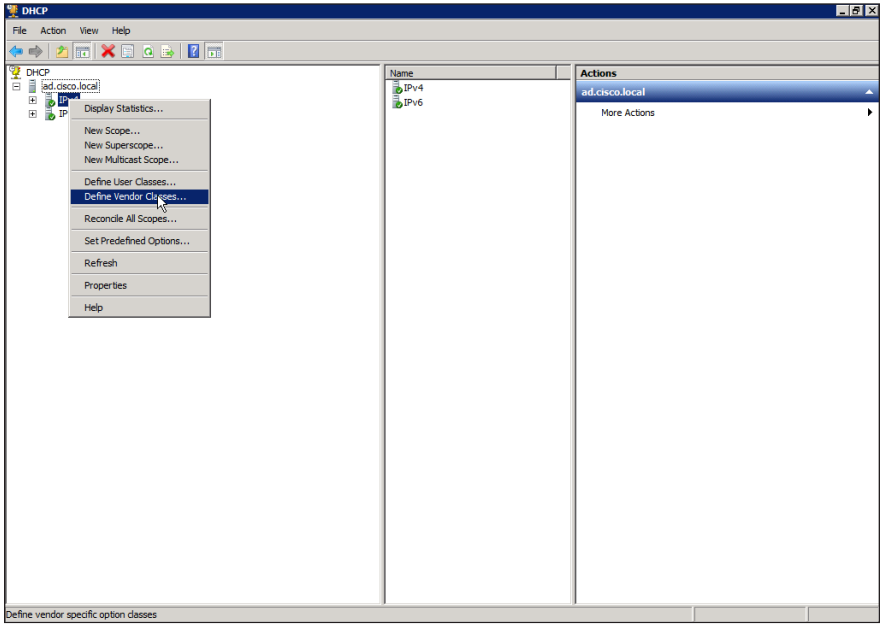
This procedure shows how the Windows DHCP server is configured to return vendor-specific information to the lightweight Cisco Aironet 1040 and 2600 Series Access Points used in this deployment guide. The vendor class identifier for a lightweight Cisco Aironet series access point is specific to each model type. To support more than one access point model, you must create a vendor class for each model type.

Table 5 - Vendor class identifiers

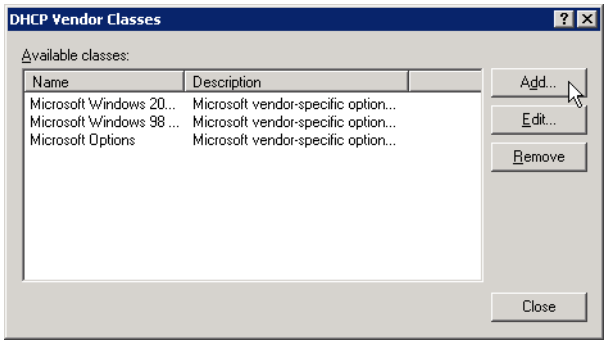
Access point	Vendor class identifier
Cisco Aironet 1040 Series	Cisco AP c1040
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600

Step 1: Open the DHCP Server Administration Tool or MMC.

Step 2: Right-click the DHCP root > IPv4, and then click **Define Vendor Classes**.



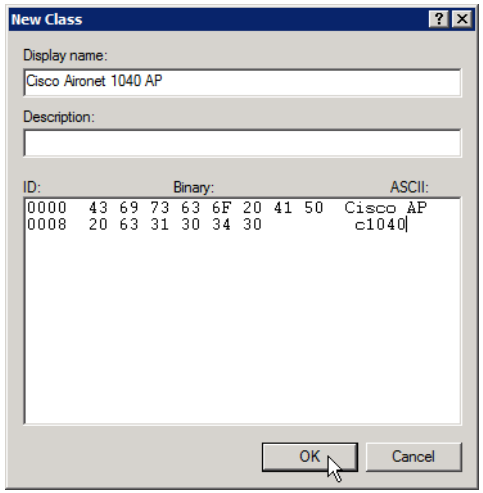
Step 3: In the **DHCP Vendor Classes** dialog box, click **Add**.



Step 4: In the New Class dialog box, enter a **Display Name**. (Example: Cisco Aironet 1040 AP)

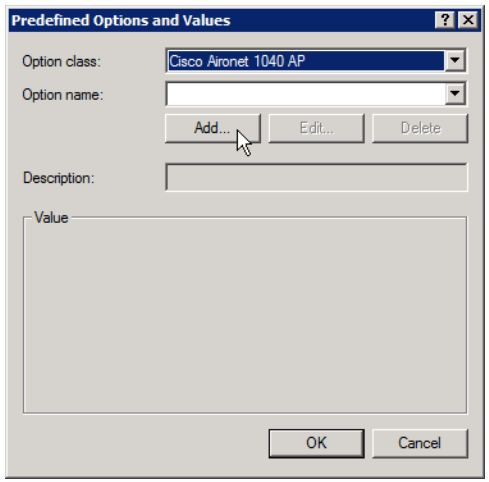
Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 3, and then click **OK**. (Example: Cisco AP c1040)

Step 6: In the DHCP Vendor Classes dialog box, click **Close**.



Step 7: Right-click the **DHCP Server Root(IPv4)**, and then choose **Set Predefined Options**.

Step 8: In the **Option Class** list, choose the class created in Step 4, and then click **Add**.

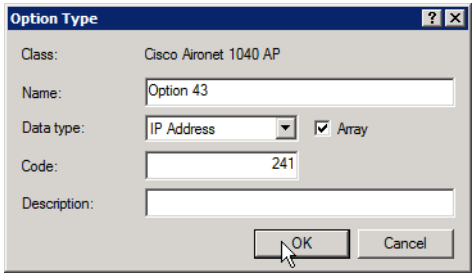


Step 9: In the **Option Type** dialog box, enter a **Name**. (Example: Option 43)

Step 10: In the **Data Type** list, choose **IP Address**.

Step 11: Select **Array**.

Step 12: In the **Code** box, enter **241**, and then click **OK**.



The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

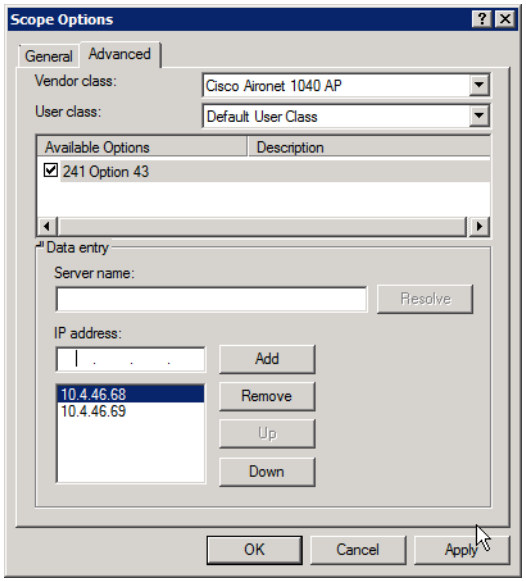
Step 13: Choose the appropriate DHCP scope. Right-click **Scope Options**, and choose **Configure Options**.

Step 14: Click the **Advanced** tab, and in the **Vendor class** list choose the class created in Step 4.

Step 15: Under **Available Options**, select **241 Option 43**.

Step 16: In the **IP address** box, enter the IP address of the primary controller's management interface, and then click **Add**. (Example: 10.4.46.68)

Step 17: Repeat Step 16 for the resilient controller, and then click **Apply**. (Example: 10.4.46.69)



Procedure 13 Configure the remote-site router

Remote-site routers require additional configuration to support wireless VLANs. The procedure varies by the number of WAN routers deployed at the remote site.

Option 1. Single WAN remote-site router

Step 1: Create wireless data and voice subinterfaces on the router's interface that connects to the access layer switch. The interface will be a physical interface when the connection is a single link, and a logical port-channel interface when the connection is EtherChannel.

```
interface GigabitEthernet0/2.65
 description Wireless Data
 encapsulation dot1Q 65
 ip address 10.5.42.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.70
 description Wireless Voice
 encapsulation dot1Q 70
 ip address 10.5.43.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

Step 2: If application optimization is deployed at the remote site as described in the *Cisco SBA—Borderless Networks Application Optimization Deployment Guide*, configure Web Cache Communication Protocol (WCCP) redirection on the router's wireless data interface.

```
interface GigabitEthernet0/2.65
 description Wireless Data
 ip wccp 61 redirect in
```

Step 3: If the network does not have a central-site DHCP server, configure the Cisco IOS Software DHCP service on the router.

```
ip dhcp excluded-address 10.5.42.1 10.5.42.10
ip dhcp excluded-address 10.5.43.1 10.5.43.10
ip dhcp pool WLAN-Data
 network 10.5.42.0 255.255.255.0
 default-router 10.5.42.1
 domain-name cisco.local
 dns-server 10.4.48.10
ip dhcp pool WLAN-Voice
 network 10.5.43.0 255.255.255.0
 default-router 10.5.43.1
 domain-name cisco.local
 dns-server 10.4.48.10
```

Option 2. Dual WAN remote-site routers

Step 1: On the primary router, create wireless data and voice subinterfaces on the interface that connects to the access layer switch. The interface will be a physical interface when the connection is a single link, and a logical port-channel interface when the connection is EtherChannel.

```
interface GigabitEthernet0/2.65
 description Wireless Data
 encapsulation dot1Q 65
 ip address 10.5.42.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.42.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string cisco123
 standby 1 track 50 decrement 10
!
interface GigabitEthernet0/2.70
 description Wireless Voice
 encapsulation dot1Q 70
 ip address 10.5.43.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.43.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string cisco123
 standby 1 track 50 decrement 10
```

Step 2: On the secondary router, create wireless data and voice subinterfaces on the interface that connects to the access layer switch. The interface will be a physical interface when the connection is a single link, and a logical port-channel interface when the connection is EtherChannel.

```
interface GigabitEthernet0/2.65
 description Wireless Data
 encapsulation dot1Q 65
 ip address 10.5.42.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.42.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string cisco123
!
interface GigabitEthernet0/2.70
 description Wireless Voice
 encapsulation dot1Q 70
 ip address 10.5.43.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.43.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string cisco123
```

Step 3: If application optimization is deployed at the remote site as described in the *Cisco SBA—Borderless Networks Application Optimization Deployment Guide*, configure WCCP redirection on both the primary and secondary router.

```
interface GigabitEthernet0/2.65
 description Wireless Data
 ip wccp 61 redirect in
```

Procedure 14 Configure the remote-site switch for APs

Before remote-site switches can offer the appropriate trunk behavior to access points configured for Cisco FlexConnect wireless switching, you must reconfigure the switch interfaces connected to the access points. For consistency and modularity, configure all WAN remote sites that have a single access switch or switch stack with the same VLAN assignment scheme.

Step 1: On the remote-site switch, create the data and voice wireless VLANs.

```
vlan 65
 name WLAN_Data
vlan 70
 name WLAN_Voice
```

Step 2: Configure the existing interface where the router is connected to allow the wireless VLANs across the trunk. If there are two routers at the site, configure both interfaces.

```
interface GigabitEthernet 1/0/24
 switchport trunk allowed vlan add 65,70
```

Step 3: Reset the switch interface where the wireless access point will be connected to its default configuration.

```
default interface GigabitEthernet 1/0/23
```

Step 4: Configure the interface where the access point will be connected to allow a VLAN trunk for remote-site VLANs.

```
interface GigabitEthernet 1/0/23
  description FlexConnect Access Point Connection
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 64
  switchport trunk allowed vlan 64,65,70
  switchport mode trunk
  switchport port-security maximum 255
  spanning-tree portfast trunk
  macro apply EgressQoS
```

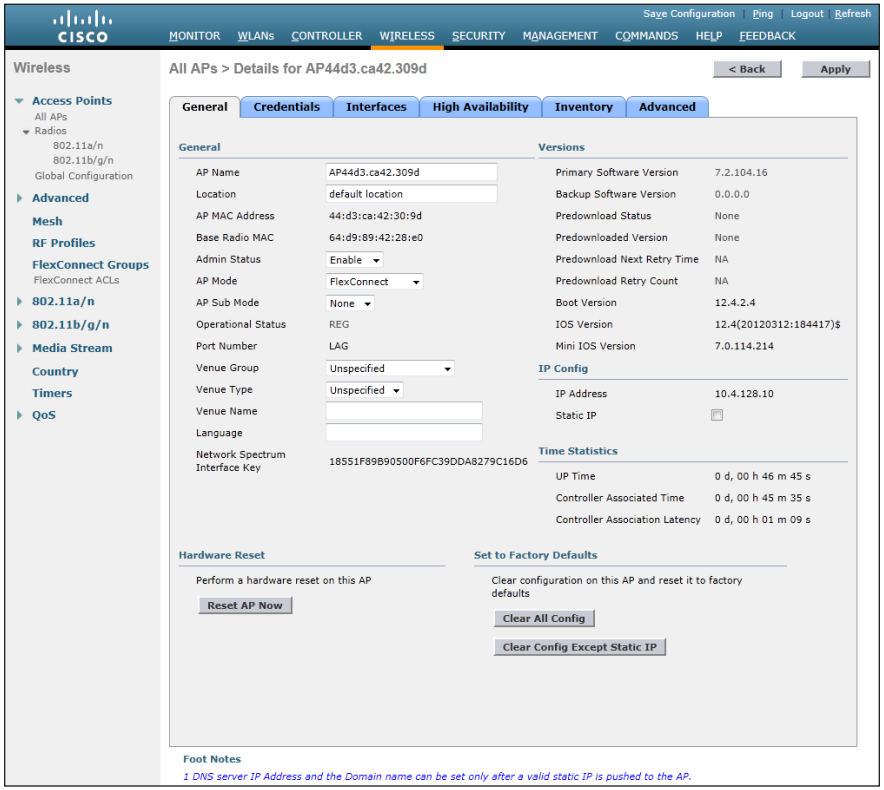
Procedure 15 Configure the AP for Cisco FlexConnect

Step 1: Connect the access point to the remote-site switch, and wait for the light on the access point to turn a solid color.

Step 2: On the Wireless LAN Controller's web interface, navigate to **Wireless** > **Access Points**.

Step 3: Select the **AP Name** of the access point you want to configure.

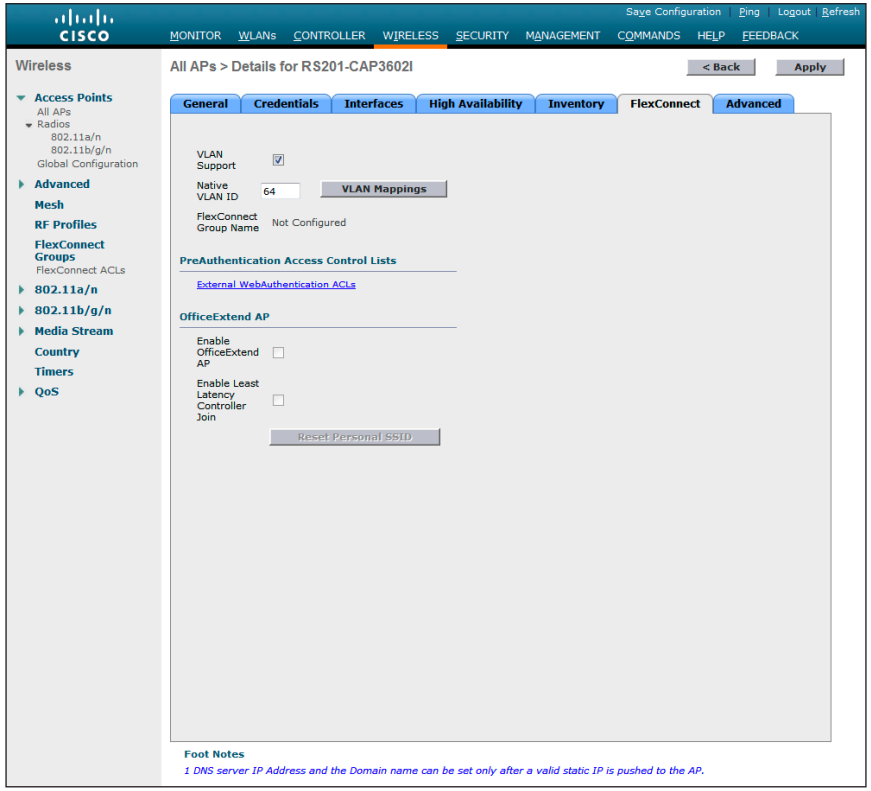
Step 4: On the General tab, in the AP Mode list, choose **FlexConnect**, and then click **Apply**. Wait for the access point to reboot and reconnect to the controller. This should take approximately three minutes.



Step 5: In **Wireless** > **Access Points**, select the same access point as in Step 3.

Step 6: On the FlexConnect tab, select **VLAN Support.**

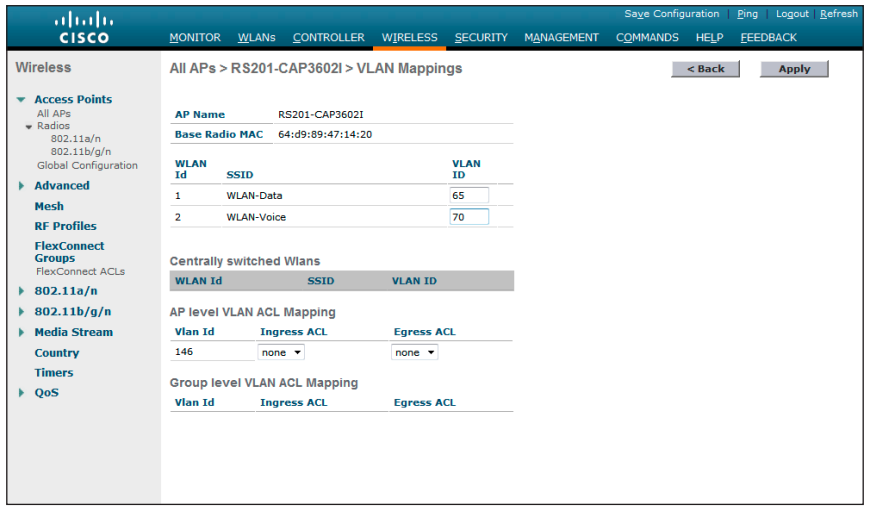
Step 7: In the **Native VLAN ID** box, enter the trunk's native VLAN number as configured in Procedure 12, and then click **Apply**. (Example: 64)



Step 8: Click **VLAN Mappings**.

Step 9: For the data WLAN, enter the VLAN number from Procedure 12 in the **VLAN ID** box. (Example: 65)

Step 10: For the voice WLAN, enter the VLAN number from Procedure 12 in the **VLAN ID** box, and then click **Apply**. (Example: 70)



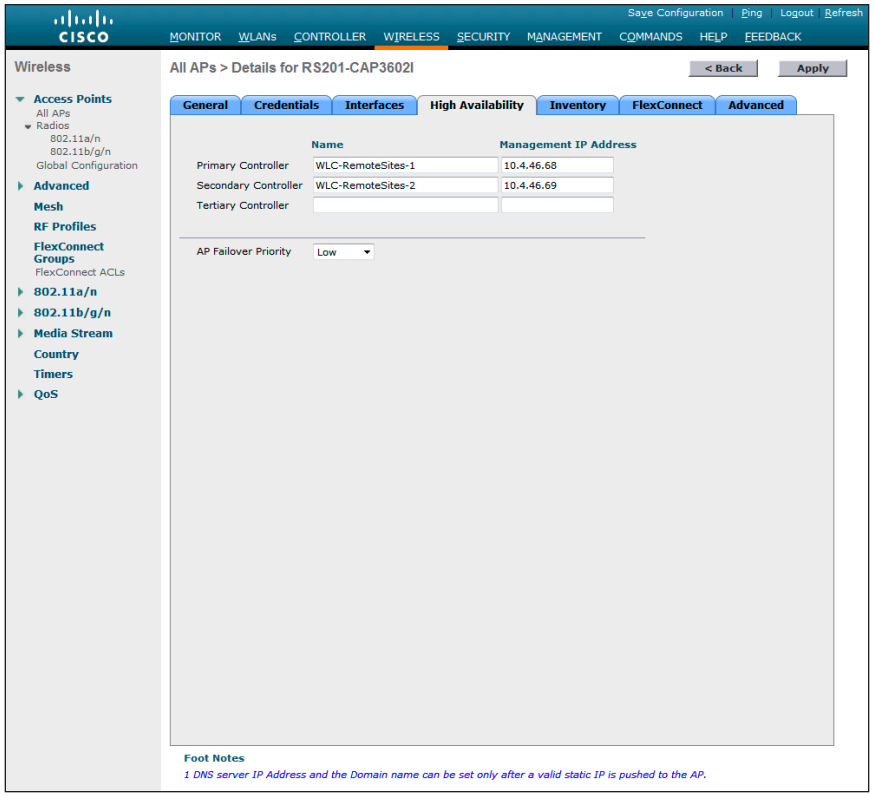
Procedure 16 Configure access points for resiliency

Step 1: On the primary WLC, navigate to **Wireless**, and select the desired access point. If the access point is not listed, check the resilient WLC.

Step 2: Click the **High Availability** tab.

Step 3: In the **Primary Controller** box, enter the name and management IP address of the primary WLC. (Example: WLC-RemoteSites-1 / 10.4.46.68)

Step 4: In the **Secondary Controller** box, enter the name and management IP address of the resilient WLC, and then click **Apply.** (Example: WLC-RemoteSites-2 / 10.4.46.69)



Procedure 17 Configure FlexConnect Groups

Step 1: On the primary WLC, navigate to **Wireless** > **FlexConnect Groups**, and then click **New**.

Step 2: In the Group Name box, enter a name that will allow you to associate the group with the remote site, and then click Apply. (Example: Remote-Site 1)

Step 3: Under Group Name, click the group you just created.

Step 4: Under Add AP, select **Select APs from current controller**.

Step 5: In the AP Name list, choose an access point that is located at the site, and then click Add.

Step 6: Repeat the previous step for every access point at the site.

Step 7: Under AAA, in the Primary Radius Server list, choose your RADIUS server, and then click Apply.

Step 8: Repeat this process for each remote site.

Process

Configuring Guest Wireless: Shared Guest Controller

1. Configure the distribution switch
2. Configure the firewall DMZ interface
3. Configure Network Address Translation
4. Configure guest network security policy
5. Create the guest wireless LAN interface
6. Configure the guest wireless LAN
7. Create the lobby admin user account
8. Create guest accounts

Procedure 1 Configure the distribution switch

The VLAN used in the following configuration examples is:

- Guest Wireless—VLAN 1128, IP: 192.168.28.0/22

Step 1: On the LAN distribution switch, for Layer 2 configuration, create the guest wireless VLAN.

```
vlan 1128
 name Guest_Wireless
```

Step 2: Configure the interfaces that connect to the Internet firewalls by adding the wireless VLAN.

```
interface GigabitEthernet1/0/24
 description IE-ASA5540a Gig0/1
!
interface GigabitEthernet2/0/24
 description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk allowed vlan add 1128
```

Step 3: Configure the interfaces that connect to the WLCs by adding the wireless VLAN.

```
interface Port-channel [WLC #1 number]
 description WLC-1 LAG
!
interface Port-channel [WLC #2 number]
 description WLC-2 LAG
!
interface range Port-channel [WLC #1 number], Port-channel
[WLC #2 number]
 switchport trunk allowed vlan add 1128
```

Procedure 2 Configure the firewall DMZ interface

Typically, the firewall DMZ is a portion of the network where traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except for specific circumstances.

The guest DMZ is connected to Cisco ASA on the appliances' internal Gigabit Ethernet interface via a VLAN trunk. The IP address assigned to the VLAN interface on the appliance is the default gateway for that DMZ subnet. The internal distribution switch's VLAN interface does not have an IP address assigned for the DMZ VLAN.

Table 6 - ASA DMZ interface information

Interface Label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet0/0.1128	192.168.28.1/22	1128	10	dmz-guests

Step 1: Login to the Internet Edge firewall using ASDM.

Step 2: Navigate to **Configuration -> Device Setup ->Interfaces.**

Step 3: On the Interface pane, click **Add** > **Interface**.

Step 4: In the Hardware Port list, choose the interface that is connected to the internal LAN distribution switch.(Example: GigabitEthernet0/0)

Step 5: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1128)

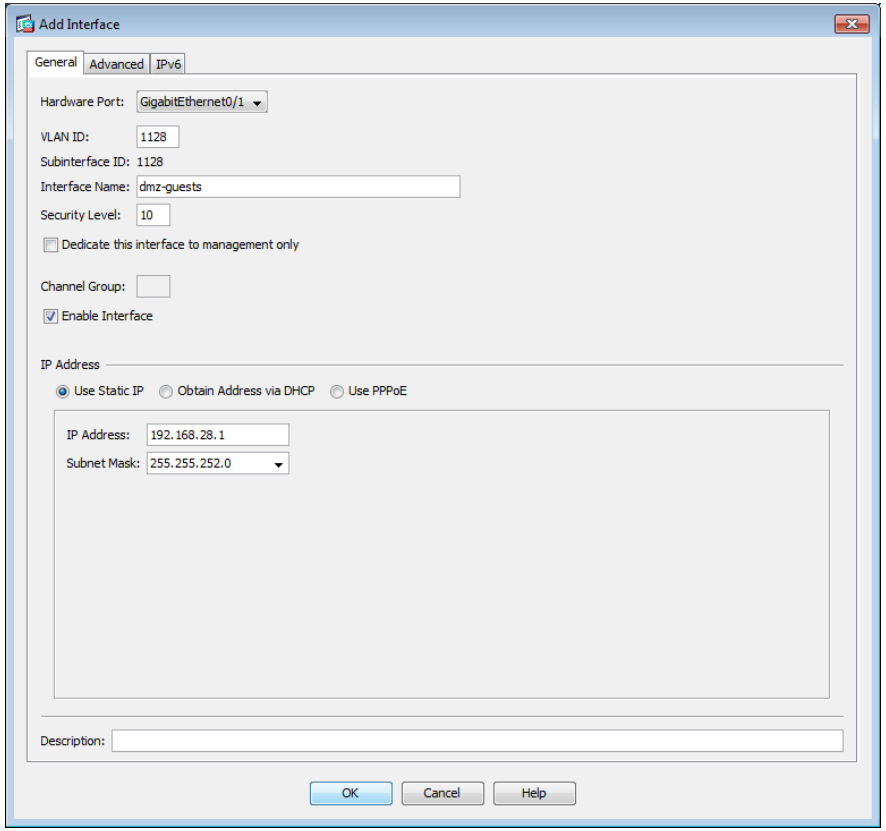
Step 6: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1128)

Step 7: Enter an **Interface Name**. (Example: dmz-guests)

Step 8: In the **Security Level** box, enter a value of **10**.

Step 9: Enter the interface **IP Address**. (Example: 192.168.28.1)

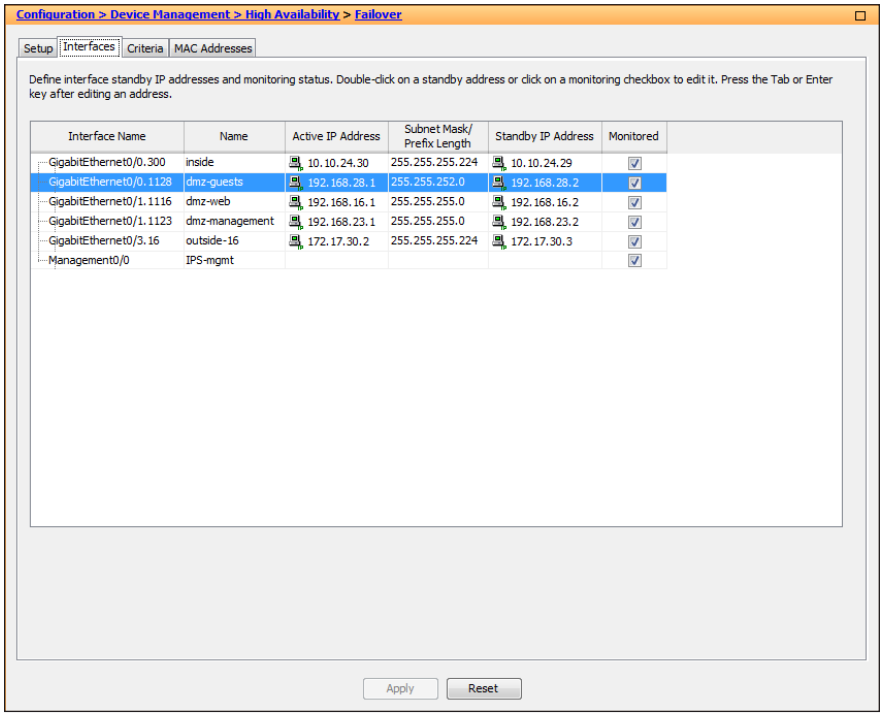
Step 10: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.252.0)



Step 11: Navigate to **Configuration > Device Management > High Availability > Failover.**

Step 12: On the Interfaces tab, in the **Standby IP address** column, enter the IP address of the standby unit for the interface you just created. (Example: 192.168.28.2)

Step 13: Select **Monitored**, and then click **Apply**.



Step 14: At the bottom of the window, click **Apply**. This saves the configuration.

Procedure 3 Configure Network Address Translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet-routable, so the firewall must translate the DMZ address of the guest clients to an outside public address.

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Step 2: Click **Add > Network Object**.

Step 3: In the Add Network Object dialog box, in the **Name** box, enter a description for the guest network. (Example: dmz-guests-network-ISPa)

Step 4: In the Type list, choose **Network**.

Step 5: In the **IP Address** box, enter the guest DMZ network address. (Example: 192.168.28.0)

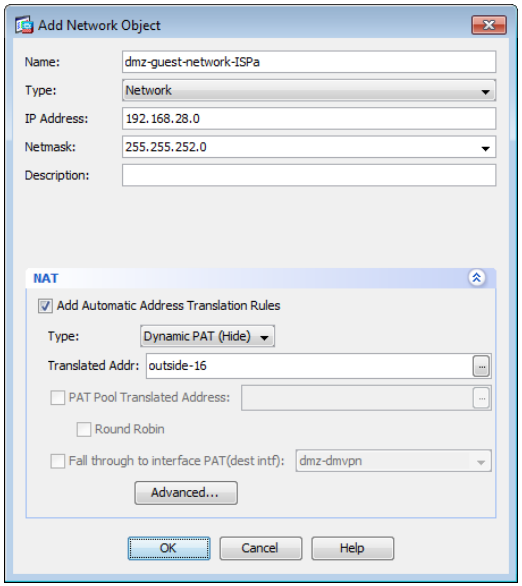
Step 6: Enter the guest DMZ netmask. (Example: 255.255.252.0)

Step 7: Click the two down arrows to expand the NAT pane.

Step 8: Select **Add Automatic Address Translation Rules**.

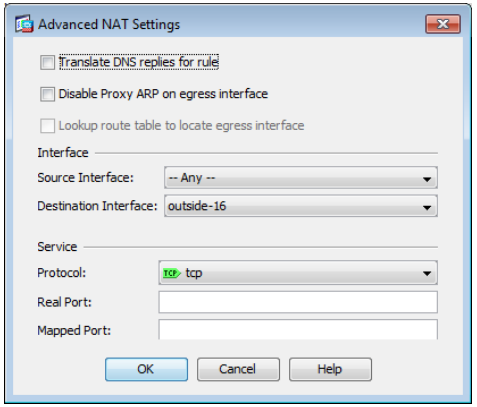
Step 9: In the Type list, choose **Dynamic PAT (Hide)**.

Step 10: In the Translated Addr list, choose the interface name for the primary Internet connection. (Example: outside-16)



Step 11: Click **Advanced**.

Step 12: In the Destination Interface list, choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)



Procedure 4 Configure guest network security policy

Step 1: Navigate to **Configuration > Firewall > Access Rules**.

Step 2: Click the rule that denies traffic from the DMZ toward other networks.

First, you enable the guests to communicate with the DNS and DHCP servers in the data center.

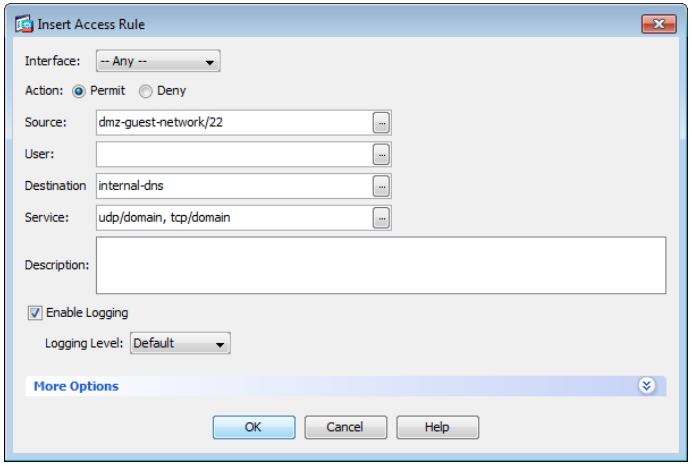
Step 3: Click **Add > Insert**.

Step 4: In the Interface list choose **Any.**

Step 5: In the Source list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 6: In the Destination list, choose the network object for the DNS server. (Example: internal-dns)

Step 7: In the Service list, enter **udp/domain, tcp/domain**, and then click **OK**.



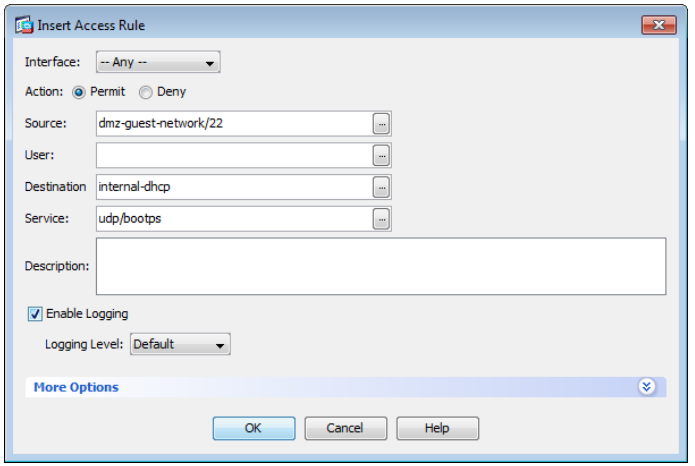
Step 8: Click **Add** > **Insert**.

Step 9: In the Interface list, choose **Any.**

Step 10: In the Source list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 11: In the Destination list, choose the network object for the DHCP server. (Example: internal-dhcp)

Step 12: In the Service list, enter **udp/bootps**, and then click **OK**.



Next, you enable the guests to communicate with the web servers in the DMZ.

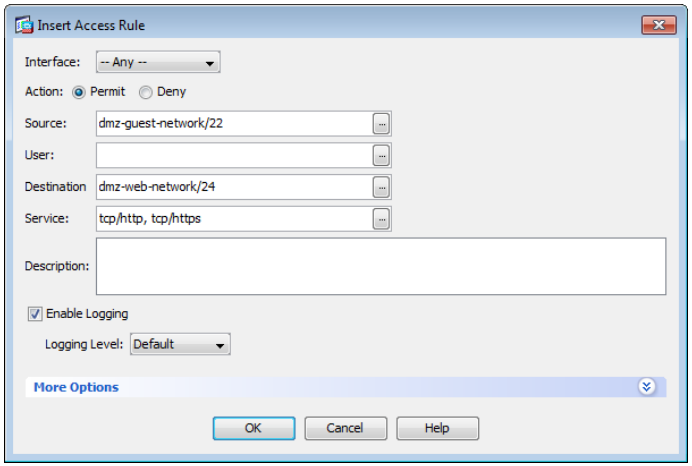
Step 13: Click **Add** > **Insert**.

Step 14: In the Interface list, choose **Any.**

Step 15: In the Source list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 16: In the Destination list, select the network object automatically created for the web DMZ. (Example: dmz-web-network/24)

Step 17: In the Service list, enter **tcp/http, tcp/https**, and then click **OK**.



Next, you remove the guest's ability communicate with other internal and DMZ devices.

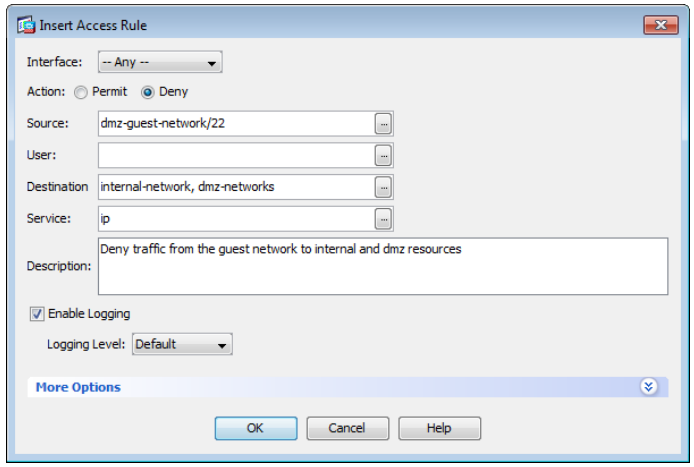
Step 18: Click **Add** > **Insert**.

Step 19: In the Interface list, choose **Any.**

Step 20: To the right of Action, select **Deny**.

Step 21: In the Source list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 22: In the Destination list, choose the network objects for the internal and DMZ networks, and then click **OK**. (Example: internal-network, dmz-networks)

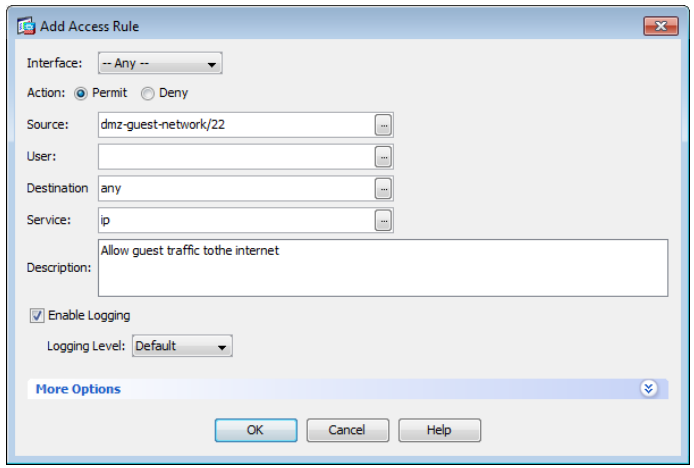


Finally, you enable the guests to communicate with the Internet.

Step 23: Click **Add** > **Insert**.

Step 24: In the Interface list, choose **Any.**

Step 25: In the Source list, select the network object automatically created for the guest DMZ, click **OK**, and then click **Apply**. (Example: dmz-guests-network/22)



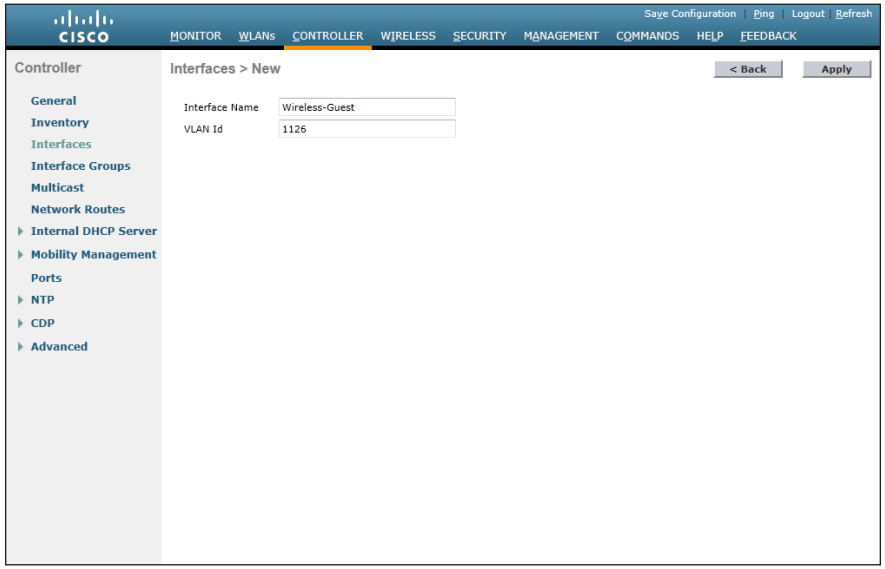
Procedure 5 Create the guest wireless LAN interface

The guest wireless interface is connected to the DMZ of the Cisco ASA 5500 Series security appliance. This allows guest wireless traffic only to and from the Internet. All traffic, regardless of the controller that the guest initially connects to, is tunneled to the guest WLC and leaves the controller on this interface. To easily identify the guest wireless devices on the network, use an IP address range for these clients that is not part of your organization's regular network. Use this procedure to add an interface that allows devices on the guest wireless network to communicate with the Internet.

Step 1: In **Controller>Interfaces,** click **New**

Step 2: Enter the **Interface Name**. (Example: Wireless-Guest)

Step 3: Enter the **VLAN identifier**, and then click **Apply**. (Example: 1128)

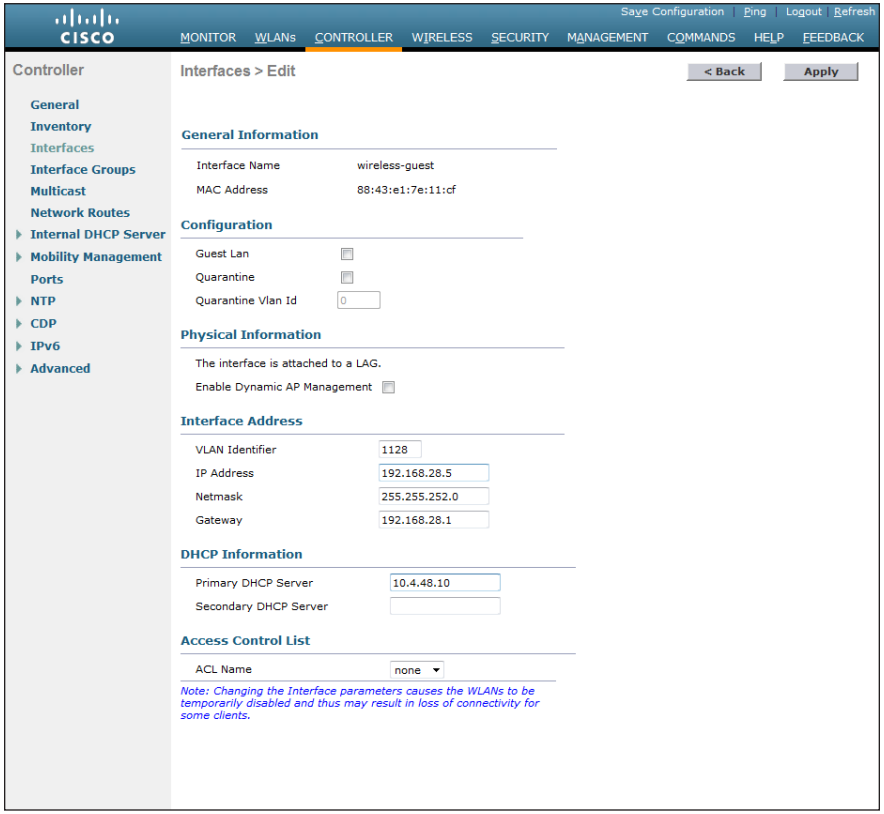


Step 4: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 192.168.28.5)

Step 5: Enter the **Netmask**. (Example: 255.255.252.0)

Step 6: In the **Gateway** box, enter the IP address of the firewall's DMZ interface defined in Procedure 2. (Example: 192.168.28.1)

Step 7: In the **Primary DHCP Server** box, enter the IP address of your organization's DHCP server, and then click **Apply**. (Example: 10.4.48.10)



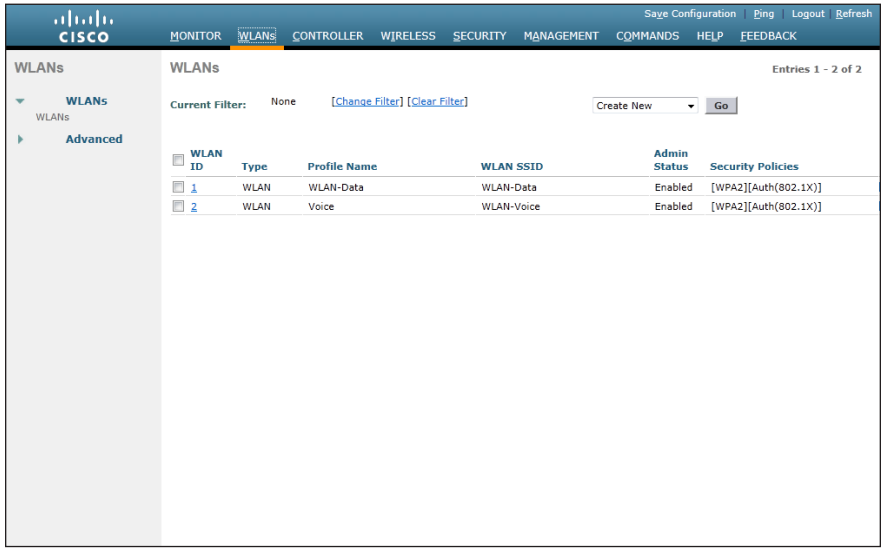
Tech Tip

To prevent DHCP from assigning addresses to wireless clients that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Procedure 6 Configure the guest wireless LAN

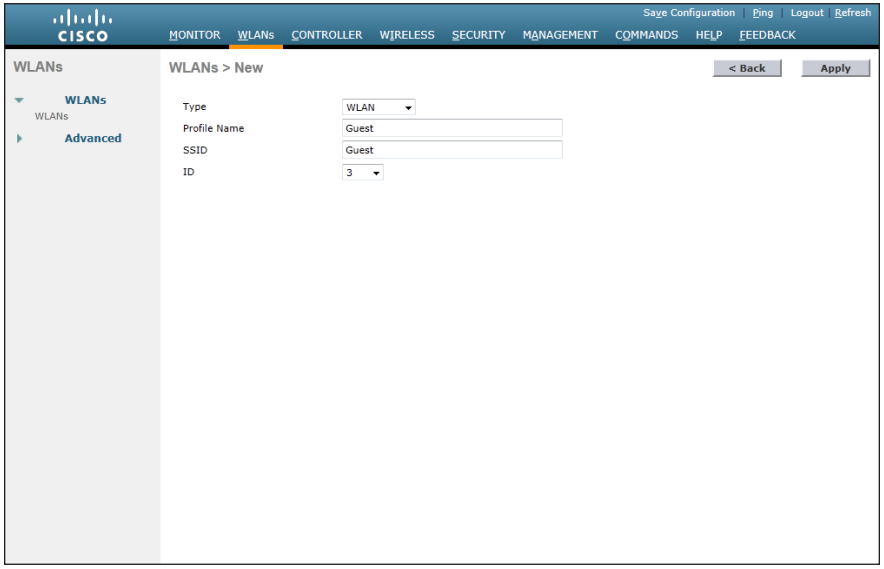
Step 1: Navigate to **WLANs**.

Step 2: In the drop-down list, choose **Create New**, and then click **Go**.

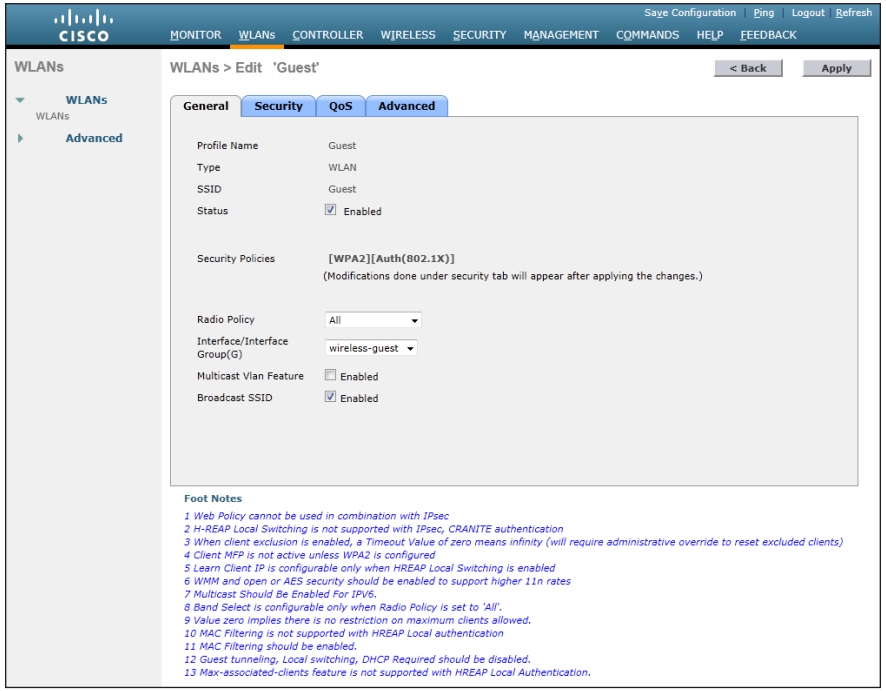


Step 3: Enter the **Profile Name**. (Example: Guest)

Step 4: In the **SSID** box, enter the guest WLAN name, and then click **Apply**. (Example: Guest)

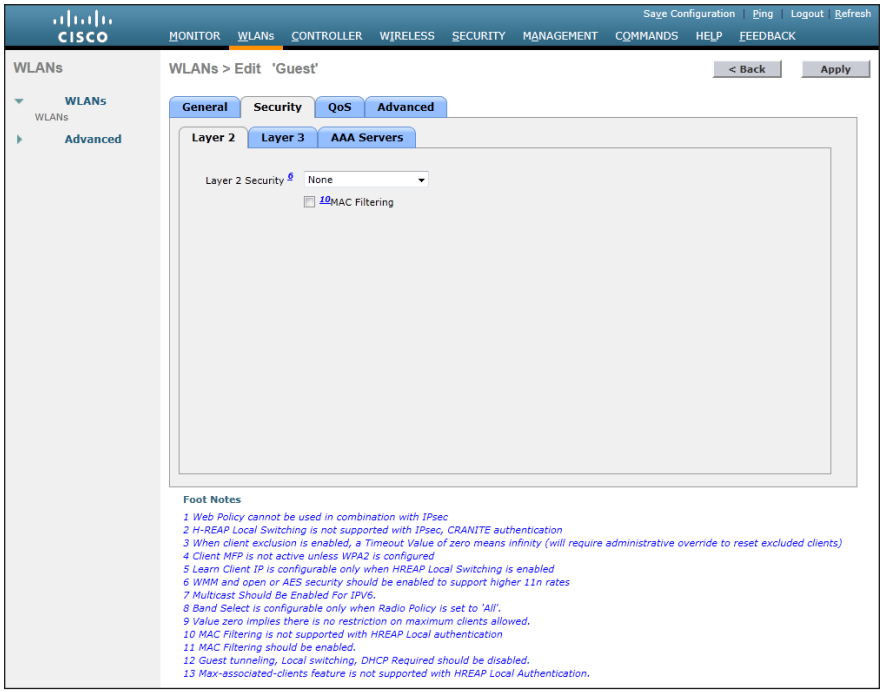


Step 5: On the General tab, in the Interface list, choose the interface created in Procedure 5. (Example: Wireless-Guest)

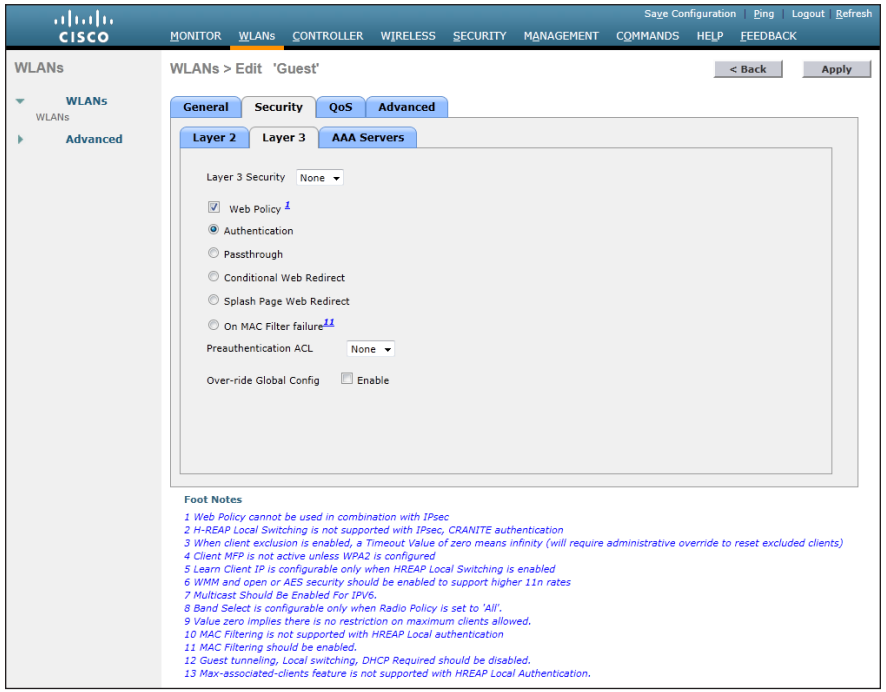


Step 6: Click the **Security** tab.

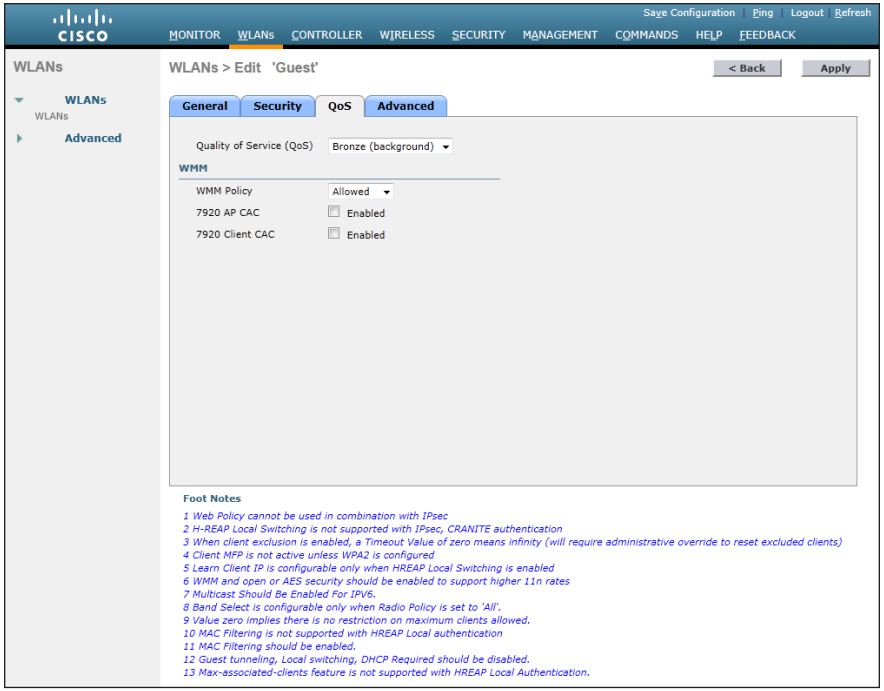
Step 7: On the Layer 2 tab in the Layer 2 Security list, choose **None**.



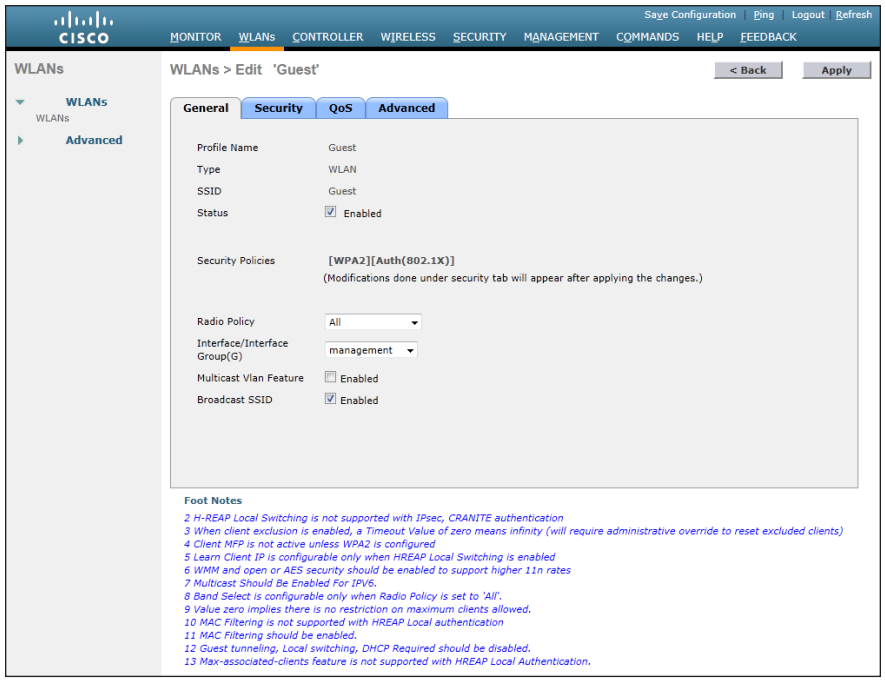
Step 8: On the Layer 3 tab, select **Web Policy**, and then click **OK**.



Step 9: On the QoS tab, in the Quality of Service (QoS) list, choose **Bronze (Background)**, and then click **Apply**.



Step 10: On the General tab, to the right of Status, select **Enabled**, and then click **Apply**.



Procedure 7 Create the lobby admin user account

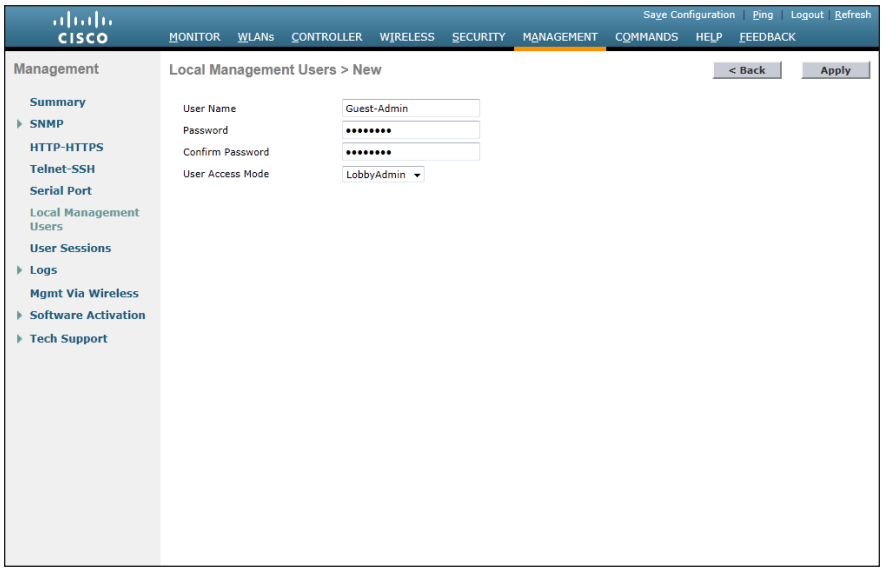
Typically, the lobby administrator is the first person to interact with your corporate guests. The lobby administrator can create individual guest user accounts and passwords that last from one to several days, depending upon the length of stay for each guest.

Step 1: In **Management** > **Local Management Users**, click **New**.

Step 2: Enter the username. (Example: Guest-Admin)

Step 3: Enter and confirm the password. (Example: C1sco123)

Step 4: In the User Access Mode list, choose **LobbyAdmin**, and then click **Apply**.

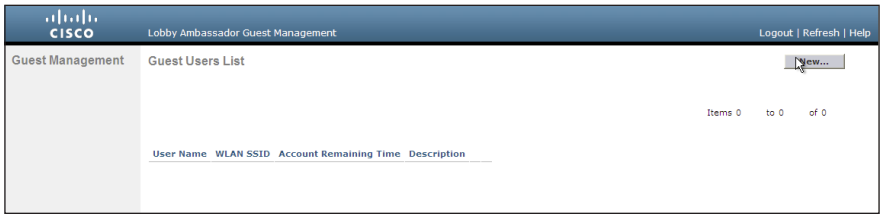


Procedure 8 Create guest accounts

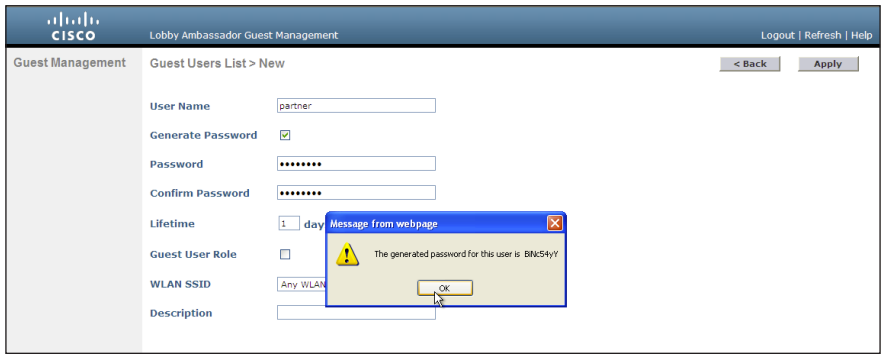
Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

Step 1: Using a web browser, open the WLC's web interface (for example, https://wlc-1.cisco.local/), and then log in using your LobbyAdmin account with the username Guest-Admin and password C1sco123.

Step 2: From the Lobby Ambassador Guest Management page, click **New**.



Step 3: Create a new username and password, or allow the system to create a password automatically by selecting **Generate Password**.



With a wireless client, you can now test connectivity to the Guest WLAN. Without any security enabled, you should receive an IP address, and—after opening a web browser—be redirected to a web page to enter a username and password for Internet access, which will be available to a guest user for 24 hours.

Process

Configuring Guest Wireless: Dedicated Guest Controller

1. Configure the DMZ switch
2. Configure the firewall DMZ interface
3. Configure Network Address Translation
4. Create network objects
5. Configure WLC security policy
6. Configure guest network security policy
7. Configure the WLC platform
8. Configure the time zone
9. Configure SNMP
10. Limit what networks can manage the WLC
11. Configure management authentication
12. Create the guest wireless LAN interface
13. Configure the guest wireless LAN
14. Configure mobility groups
15. Create the lobby admin user account
16. Configure the internal WLCs for a guest
17. Create guest accounts

Procedure 1 Configure the DMZ switch

The VLANs used in the following configuration examples are:

- Guest Wireless—VLAN 1128, IP: 192.168.28.0/22
- Wireless management—VLAN 1119, IP 192.168.19.0/24

Step 1: On the DMZ switch, create the wireless VLANs .

```
vlan 1119
 name WLAN_Mgmt
vlan 1128
 name Guest_Wireless
```

Step 2: Configure the interfaces that connect to the Internet firewalls as trunk ports and add the wireless VLANs.

```
interface GigabitEthernet1/0/24
 description IE-ASA5545a Gig0/1
!
interface GigabitEthernet2/0/24
 description IE-ASA5545b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan add 1119, 1128
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

Step 3: Configure EtherChannel member interfaces.

This deployment uses Layer 2 EtherChannels to connect the WLCs to the DMZ switch. Connect the WLC EtherChannel uplinks to separate devices in the DMZ stack.

On the DMZ switch, the physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is best if they are added in multiples of two.

```
interface GigabitEthernet 1/0/1
 description DMZ-WLC-Guest-1 Port 1
!
interface GigabitEthernet 2/0/1
 description DMZ-WLC-Guest-1 Port 2
!
interface range GigabitEthernet 1/0/1, GigabitEthernet 2/0/1
 channel-group 12 mode on
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

Step 4: Configure trunks.

An 802.1Q trunk is used for the connection to the WLC, which allows the firewall to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are reduced to only the VLANs that are active on the WLC.

```
interface Port-channel12
 description DMZ-WLC-Guest
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1119,1128
 switchport mode trunk
 logging event link-status
 no shutdown
```

Procedure 2 Configure the firewall DMZ interface

Typically, the firewall DMZ is a portion of the network where traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except for specific circumstances.

The various DMZ networks are connected to Cisco ASA on the appliances' Gigabit Ethernet interface via a VLAN trunk. The IP address assigned to the VLAN interface on the appliance is the default gateway for that DMZ subnet. The DMZ switch's VLAN interface does not have an IP address assigned for the DMZ VLAN.

Table 7 - ASA DMZ interface information

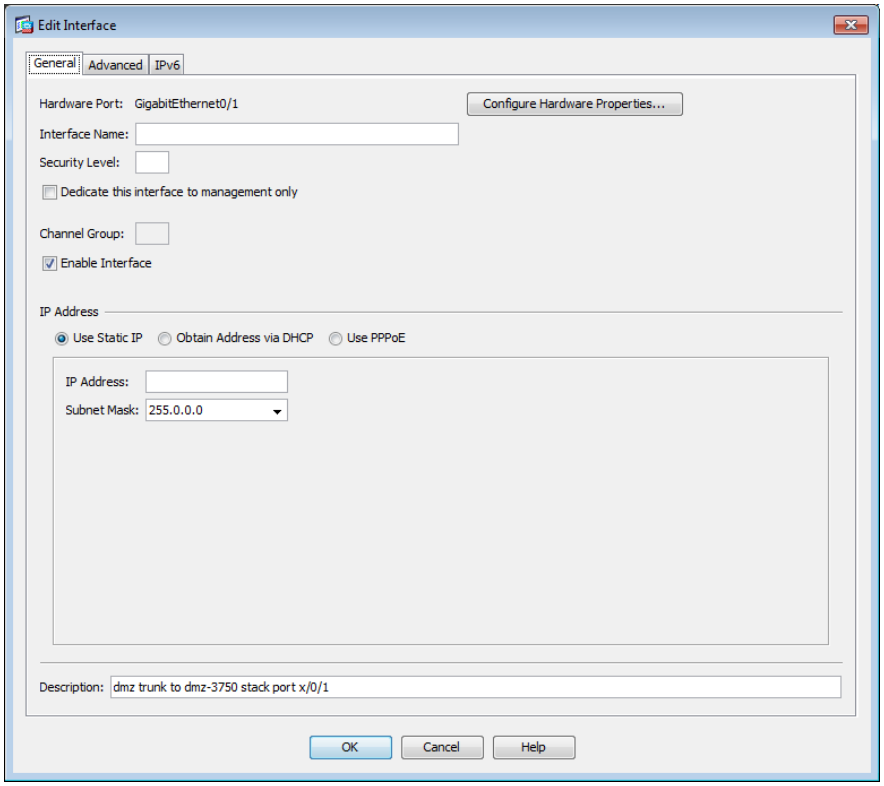
Interface Label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet0/1.1119	192.168.19.1/24	1119	50	dmz-wlc
GigabitEthernet0/1.1128	192.168.28.1/22	1128	10	dmz-guests

Step 1: Login to the Internet Edge firewall using ASDM.

Step 2: In **Configuration** > **Device Setup** > **Interfaces**, click the interface that is connected to the DMZ switch. (Example: GigabitEthernet0/1)

Step 3: Click **Edit**.

Step 4: Select **Enable Interface**, and then click **OK**.



Step 5: On the Interface pane, click **Add** > **Interface**.

Step 6: In the Hardware Port list, choose the interface configured in Step1. (Example: GigabitEthernet0/1)

Step 7: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

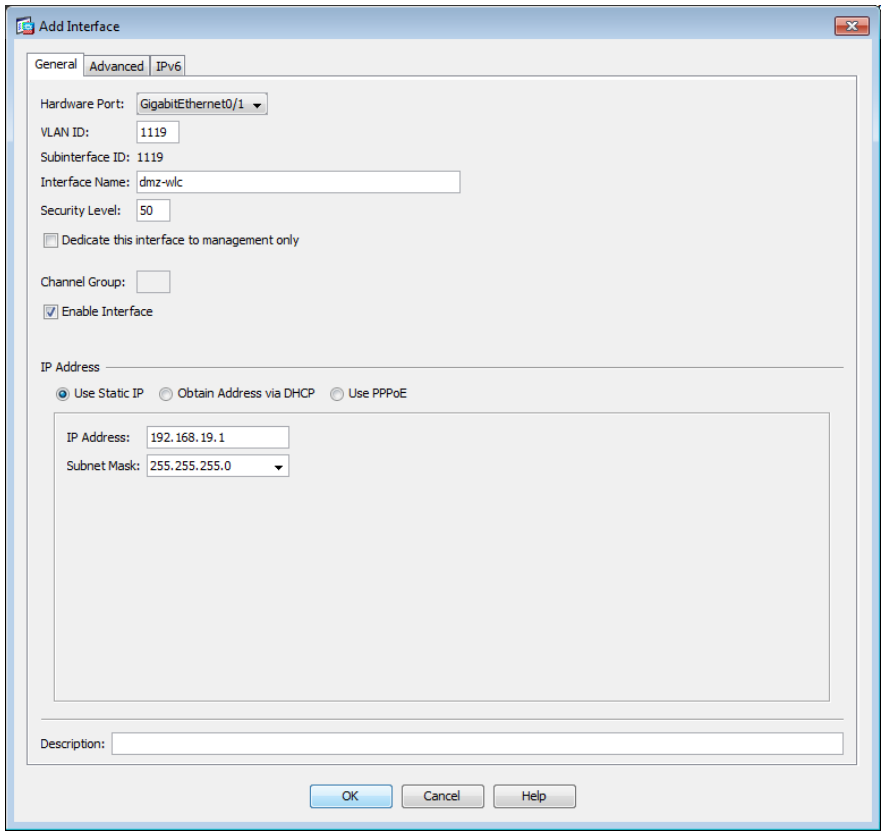
Step 8: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

Step 9: Enter an **Interface Name**. (Example: dmz-wlc)

Step 10: In the **Security Level** box, enter a value of **50**.

Step 11: Enter the interface **IP Address**. (Example: 192.168.19.1)

Step 12: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)



Step 13: Repeat Step 5 through Step 12 for the dmz-guests interface.

Procedure 3 Configure Network Address Translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet-routable, so the firewall must translate the DMZ address of the guest clients to an outside public address.

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Step 2: Click **Add > Network Object**.

Step 3: In the Add Network Object dialog box, in the **Name** box, enter a description for the guest network. (Example: dmz-guests-network-ISPa)

Step 4: In the Type list, choose **Network**.

Step 5: In the **IP Address** box, enter the guest DMZ network address. (Example: 192.168.28.0)

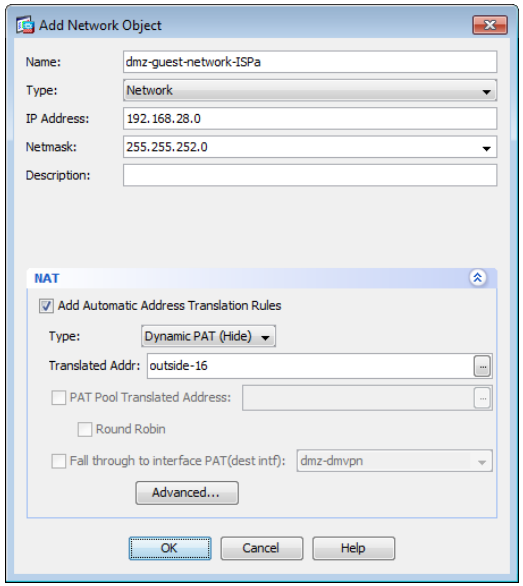
Step 6: Enter the guest DMZ netmask. (Example: 255.255.252.0)

Step 7: Click the two down arrows to expand the NAT pane.

Step 8: Select **Add Automatic Address Translation Rules**.

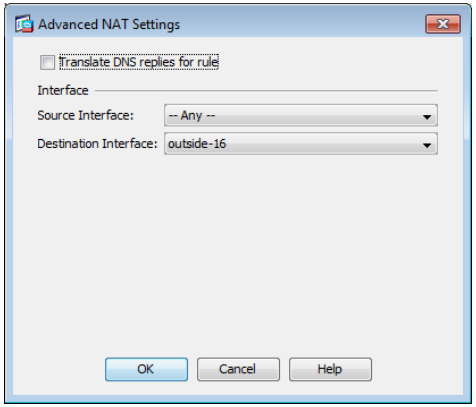
Step 9: In the Type list, choose **Dynamic PAT (Hide)**.

Step 10: In the Translated Addr list, choose the interface name for the primary Internet connection. (Example: outside-16)



Step 11: Click **Advanced**.

Step 12: In the Destination Interface list, choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)



Procedure 4 Create network objects

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

First, add a network object for the every internal WLC in your organization.

Step 2: Click **Add > Network Object**.

Step 3: In the Add Network Object dialog box, in the **Name** box, enter a description of the WLC. (Example: wlc-1)

Step 4: In the Type list, choose **Host**.

Step 5: In the **IP Address** box, enter the WLC's management interface IP address, and then click **OK**. (Example: 10.4.46.64)

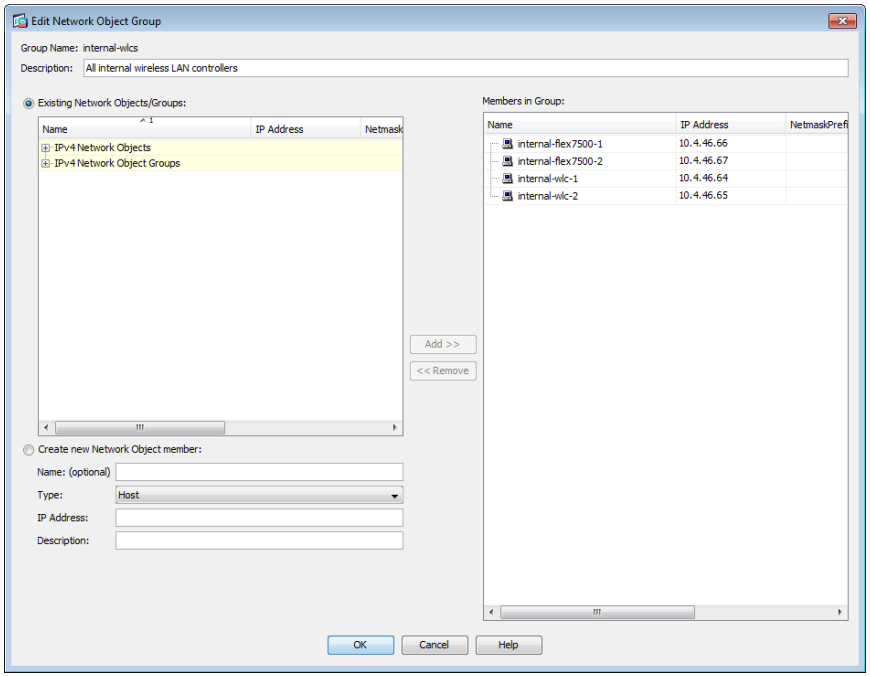
Step 6: Repeat Step 2 through Step 5 for every WLC inside your organization.

Next, to simplify security policy configuration, create a network object group that contains every WLC inside your organization

Step 7: Click **Add > Network Object Group**.

Step 8: In the Add Network Object Group dialog box, enter a name for the group in the **Group Name** box. (Example: internal-wlcs)

Step 9: Choose the every internal WLC from the Existing Network Objects/Groups pane, click **Add**, and then click **OK**.



Next, create a network object group that contains the private DMZ address of every WLC in the DMZ.

Step 10: Click **Add > Network Object Group**.

Step 11: In the Add Network Object Group dialog box, enter a name for the group in the **Group Name** box. (Example: dmz-wlcs)

Step 12: Choose the primary WLC from the Existing Network Objects/Groups pane, and then click **Add**.

Step 13: Choose the resilient WLC from the Existing Network Objects/Groups pane, click **Add**, and then click **OK**.

Procedure 5 Configure WLC security policy

Step 1: Navigate to **Configuration > Firewall > Access Rules**.

Step 2: Click the rule that denies traffic from the DMZ toward other networks.

Next, you will insert a new rule above the rule you selected that enables the WLCs in the DMZ to communicate with the AAA server in the data center for management and user authentication.

Step 3: Click **Add > Insert**.

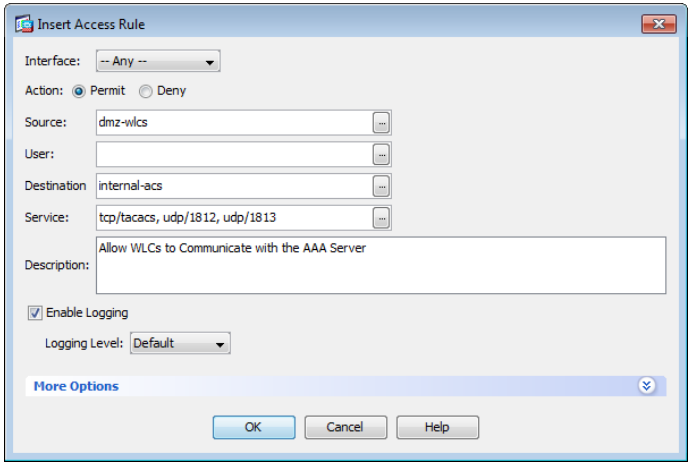
Step 4: In the Internet Access Rule dialog box, in the Interface list, select **—Any—**.

Step 5: To the right of Action, select **Permit**.

Step 6: In the Source list, choose the network object group created in Step 11 of Procedure 4, "Create network objects." (Example: dmz-wlcs)

Step 7: In the Destination list, choose the network object for the AAA Server. (Example: internal-acs)

Step 8: In the Service list, enter **tcp/tacacs, udp/1812, udp/1813**, and then click **OK**.



Next, you must enable the WLCs in the DMZ to synchronize their time with the NTP server in the data center.

Step 9: Click **Add > Insert**.

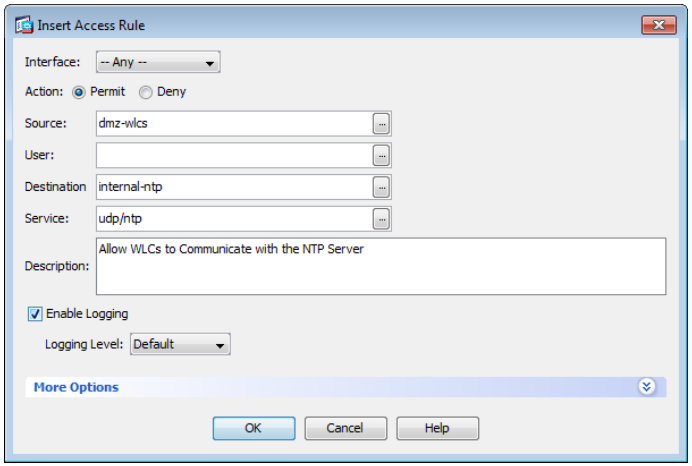
Step 10: In the Internet Access Rule dialog box, in the Interface list, select **—Any—**.

Step 11: To the right of Action, select **Permit**.

Step 12: In the Source list, choose the network object group created in Step 11 of Procedure 4, "Create network objects." (Example: dmz-wlcs)

Step 13: In the Destination list, choose the network object for the NTP Server. (Example: internal-ntp)

Step 14: In the Service list, enter **udp/ntp**, and then click **OK**.



Next, you enable the WLCs in the DMZ to be able to download new software via FTP.

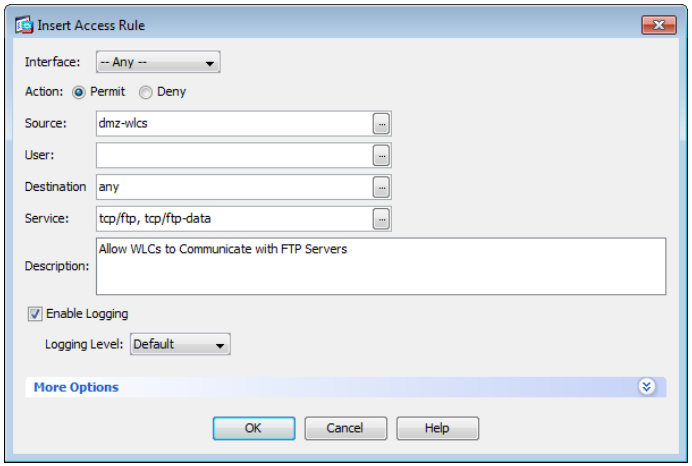
Step 15: Click **Add** > **Insert**.

Step 16: In the Internet Access Rule dialog box, in the Interface list, select **—Any—**.

Step 17: To the right of Action, select **Permit**.

Step 18: In the Source list, choose the network object group created in Step 11 of Procedure 4, "Create network objects." (Example: dmz-wlcs)

Step 19: In the Service list, enter **tcp/ftp, tcp/ftp-data**, and then click **OK**.



Now you enable the guest WLC to communicate with the WLCs inside the organization.

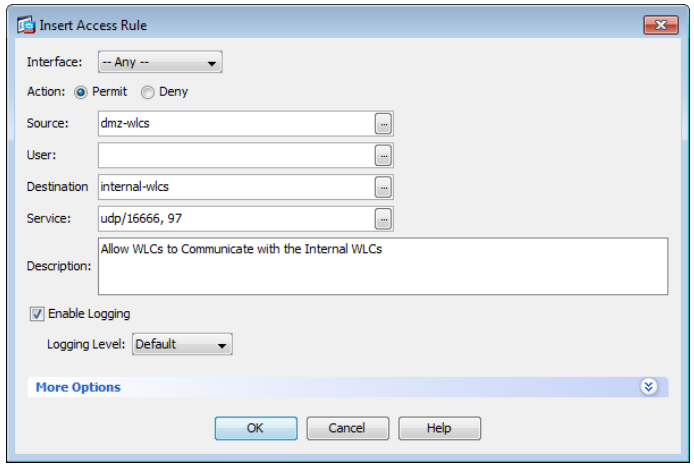
Step 20: Click **Add** > **Insert**.

Step 21: In the Interface list, choose **Any.**

Step 22: In the Source list, choose the network object group created in Step 11 of Procedure 4, "Create network objects." (Example: dmz-wlcs)

Step 23: In the Destination list, choose the network object group created in Step 8 of Procedure 4, "Create network objects." (Example: internal-wlcs)

Step 24: In the Service list, enter **udp/16666, 97**, and then click **OK**.



Finally you enable the guest WLC to communicate with the DHCP server inside your organization.

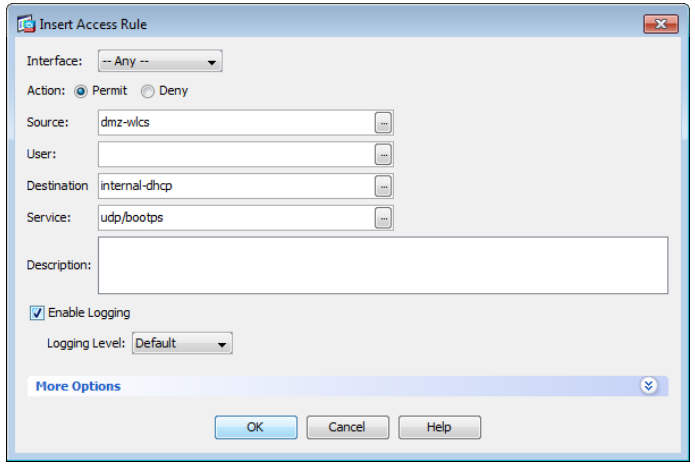
Step 25: Click **Add** > **Insert**.

Step 26: In the Interface list, choose **Any.**

Step 27: In the Source list, choose the network object group created in Step 11 of Procedure 4, "Create network objects." (Example: dmz-wlcs)

Step 28: In the Destination list, choose the network object group for the internal DHCP server. (Example: DHCP_Server_in_DC)

Step 29: In the Service list, enter **udp/bootps**, click **OK**, and then click **Apply**..



Procedure 6 Configure guest network security policy

Step 1: Navigate to **Configuration** > **Firewall** > **Access Rules**.

Step 2: Click the rule that denies traffic from the DMZ toward other networks.

First, you enable the guests to communicate with the DNS and DHCP servers in the data center.

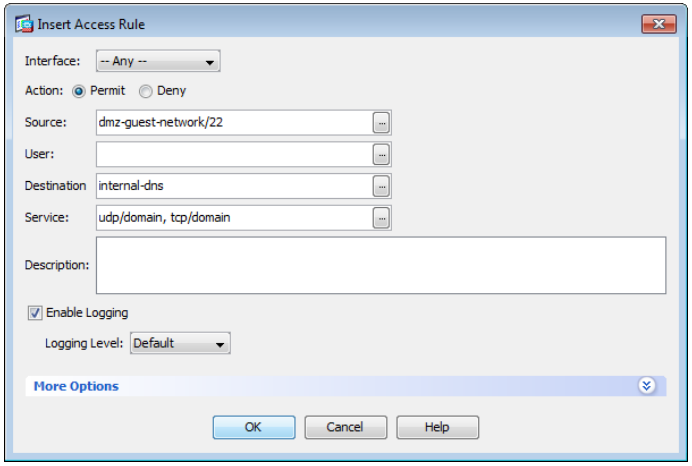
Step 3: Click **Add** > **Insert**.

Step 4: In the Interface list, choose **Any.**

Step 5: In the Source list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 6: In the Destination list, choose the network object for the DNS server. (Example: internal-dns)

Step 7: In the Service list, enter **udp/domain, tcp/domain**, and then click **OK**.



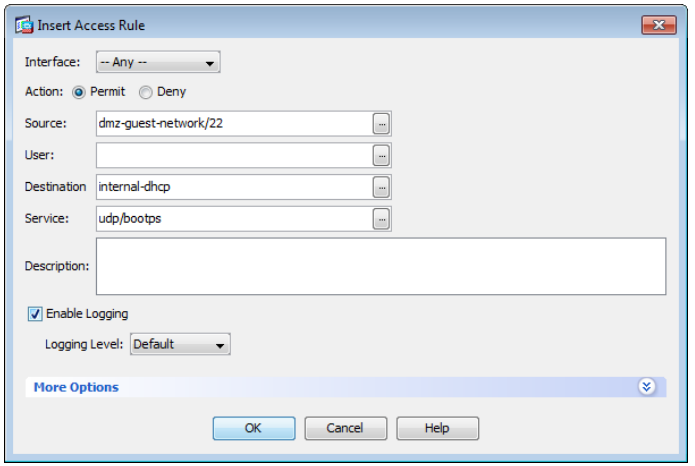
Step 8: Click **Add** > **Insert**.

Step 9: In the Interface list, choose **Any.**

Step 10: In the Source list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 11: In the Destination list, choose the network object for the DHCP server. (Example: internal-dhcp)

Step 12: In the Service list, enter **udp/bootps**, and then click **OK**.



Next, you enable the guests to communicate with the web servers in the DMZ.

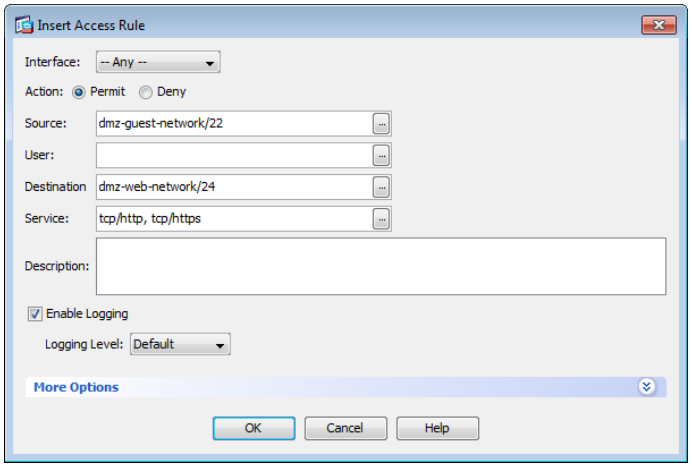
Step 13: Click **Add** > **Insert**.

Step 14: In the Interface list, choose **Any.**

Step 15: In the Source list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 16: In the Destination list, select the network object automatically created for the web DMZ. (Example: dmz-web-network/24)

Step 17: In the Service list, enter **tcp/http, tcp/https**, and then click **OK**.



Next, you remove the guest's ability communicate with other internal and DMZ devices.

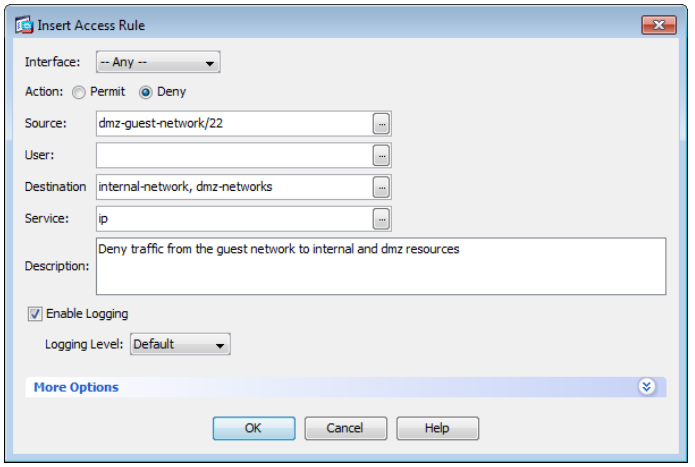
Step 18: Click **Add** > **Insert**.

Step 19: In the Interface list, choose **Any.**

Step 20: To the right of Action, select **Deny**.

Step 21: In the Source list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 22: In the Destination list, choose the network objects for the internal and DMZ networks, and then click **OK**. (Example: internal-network, dmz-networks)

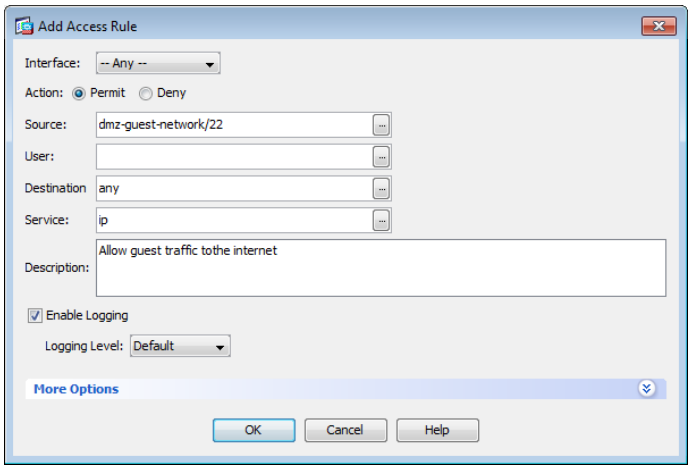


Finally, you enable the guests to communicate with the Internet.

Step 23: Click **Add** > **Insert**.

Step 24: In the Interface list, choose **Any.**

Step 25: In the Source list, select the network object automatically created for the guest DMZ, click **OK**, and then click **Apply**. (Example: dmz-guests-network/22)



Procedure 7 Configure the WLC platform

After the WLC is physically installed and powered up, you will see the following on the console:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: YES
```

Step 1: Enter a system name. (Example: GUEST-1)

```
System Name [Cisco_7e:8e:43] (31 characters max): GUEST-1
```

Step 2: Enter an administrator username and password.

Tech Tip

Use at least three of the following four classes in the password: lowercase letters, uppercase letters, digits or special characters.

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****
```

Step 3: Use DHCP for the service port interface address.

```
Service Interface IP address Configuration [none] [DHCP]: DHCP
```

Step 4: Enable the management interface.

```
Enable Link Aggregation (LAG) [yes][NO]: YES
Management Interface IP Address: 192.168.19.54
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 192.168.19.1
Management Interface VLAN Identifier (0 = untagged): 1119
```

Step 5: Enter the default DHCP server for clients. (Example: 10.4.48.10)

```
Management Interface DHCP Server IP Address: 10.4.48.10
```

Step 6: The virtual interface is used by the WLC for Mobility DHCP relay and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

```
Virtual Gateway IP Address: 192.0.2.1
```

Step 7: Enter a name that will be used as the default mobility and RF group. (Example: GUEST)

```
Mobility/RF Group Name: GUEST
```

Step 8: Enter an SSID for the WLAN that supports data traffic. You will be able to leverage this later in the deployment process.

```
Network Name (SSID): Guest
Configure DHCP Bridging Mode [yes][NO]: NO
```

Step 9: For increased security, enable DHCP snooping.

```
Allow Static IP Addresses {YES][no]: NO
```

Step 10: You will configure the RADIUS Server later by using the GUI.

```
Configure a RADIUS Server now? [YES][no]: NO
```

Step 11: Enter the correct country code for the country where you are deploying the WLC.

```
Enter Country Code list (enter 'help' for a list of countries)
[US]: US
```

Step 12: Enable all wireless networks.

```
Enable 802.11b network [YES][no]: YES
Enable 802.11a network [YES][no]: YES
Enable 802.11g network [YES][no]: YES
```

Step 13: Enable the RRM auto-RF feature. This helps you keep your network up and operational.

```
Enable Auto-RF [YES][no]: YES
```

Step 14: Synchronize the WLC clock to your organization's NTP server.

```
Configure a NTP server now? [YES][no]:YES
Enter the NTP server's IP address: 10.4.48.17
Enter a polling interval between 3600 and 604800 secs: 86400
```

Step 15: Save the configuration. If you enter **NO**, the system will restart without saving the configuration and you will have to complete this procedure again.

```
Configuration correct? If yes, system will save it and reset.
[yes][NO]: YES
Configuration saved!
Resetting system with new configuration
```

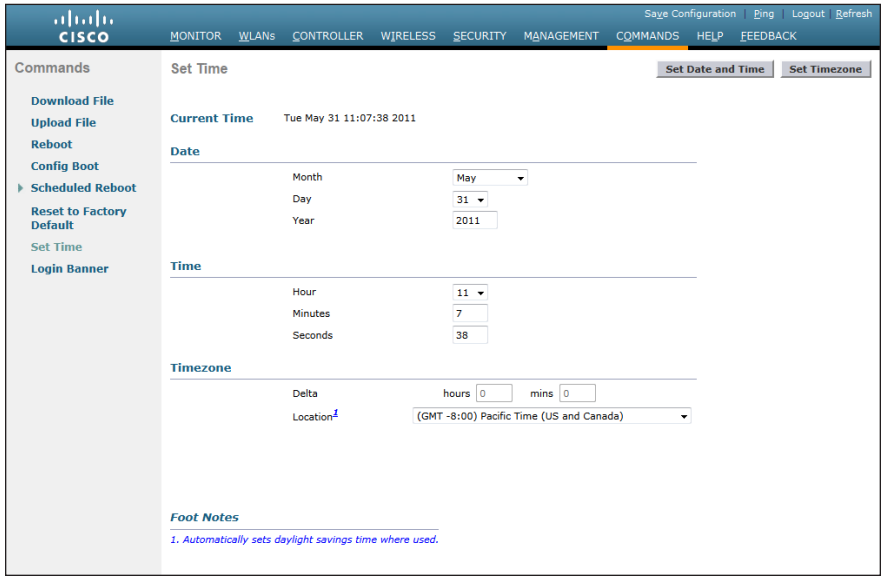
Step 16: After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page using the credentials defined in Step 2. (Example: https://guest-1.cisco.local/)

Procedure 8 Configure the time zone

Step 1: Navigate to **Commands > Set Time.**

Step 2: In the Location list, choose the time zone that corresponds to the location of the WLC.

Step 3: Click **Set Timezone**.



Procedure 9 Configure SNMP

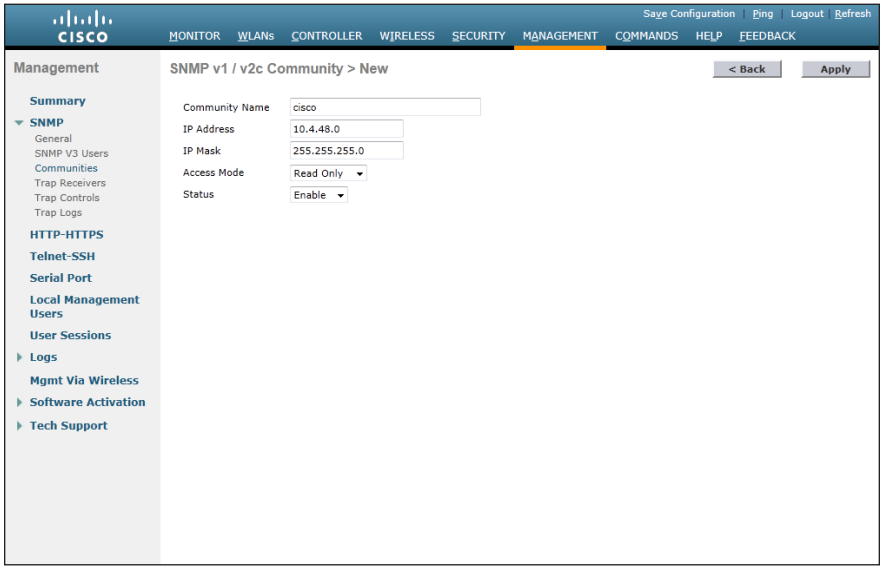
Step 1: In **Management > SNMP > Communities**, click **New**.

Step 2: Enter the **Community Name**. (Example: cisco)

Step 3: Enter the **IP Address.** (Example: 10.4.48.0)

Step 4: Enter the **IP Mask**. (Example: 255.255.255.0)

Step 5: In the Status list, choose **Enable**, and then click **Apply**.



Step 6: In **Management > SNMP > Communities**, click **New**.

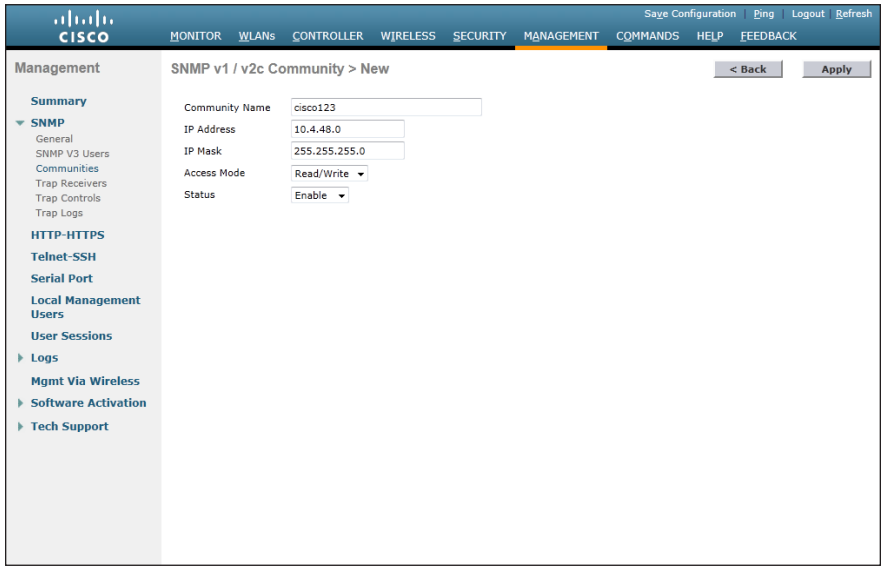
Step 7: Enter the **Community Name**. (Example: cisco123)

Step 8: Enter the **IP Address.** (Example: 10.4.48.0)

Step 9: Enter the **IP Mask**. (Example: 255.255.255.0)

Step 10: In the Access Mode list, choose **Read/Write**.

Step 11: In the Status list, choose **Enable**, and then click **Apply**.

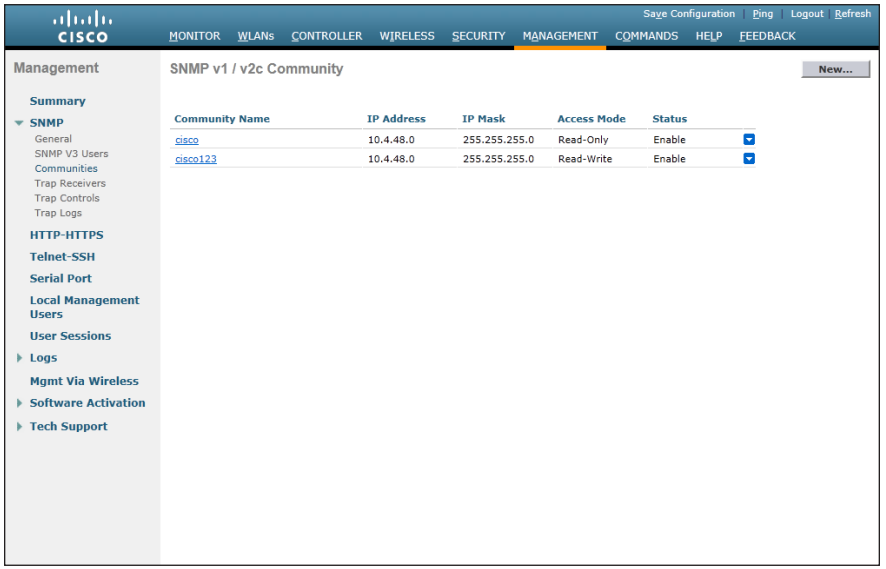


Step 12: Navigate to **Management** > **SNMP** > **Communities**.

Point to the blue box for the **public** community, and then click **Remove**.

Step 13: On the message "Are you sure you want to delete?", click **OK**.

Step 14: Repeat Step 12 and Step 13 for the **private** community.



Procedure 10 Limit what networks can manage the WLC

(Optional)

In networks where network operational support is centralized you can increase network security by using an access list to limit the networks that can access your controller. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

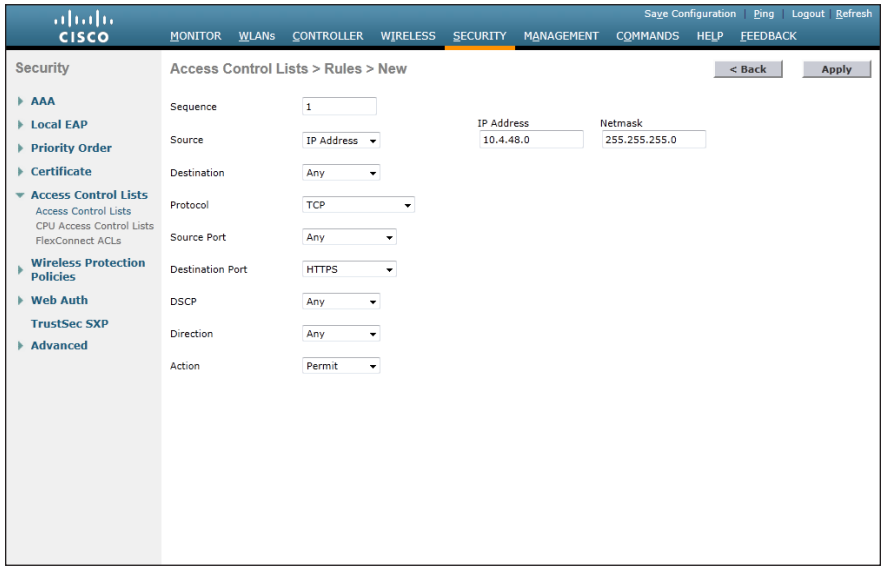
Step 1: In **Security** > **Access Control Lists** > **Access Control Lists**, click **New**.

Step 2: Enter an access list name, and then click **Apply**.

Step 3: In the list, choose the name of the access list you just created, and then click **Add New Rule**.

Step 4: In the window, enter the following configuration details, and then click **Apply**.

- Sequence — 1
- Source — 10.4.48.0 / 255.255.255.0
- Destination — Any
- Protocol — TCP
- Destination Port — HTTPS
- Action — Permit



Step 5: Repeat Step 1 through Step 4 using the configuration details in the following table.

Sequence	Source	Destination	Protocol	Destination port	Action
2	10.4.48.0/ 255.255.255.0	Any	TCP	Other/22	Permit
3	Any	Any	TCP	HTTPS	Deny
4	Any	Any	TCP	Other/22	Deny
5	Any	Any	Any	Any	Permit

Step 6: In **Security > Access Control Lists > CPU Access Control Lists**, select **Enable CPU ACL**.

Step 7: In the **ACL Name** list, choose the ACL you just created, and then click **Apply.**

Procedure 11 Configure management authentication

(Optional)

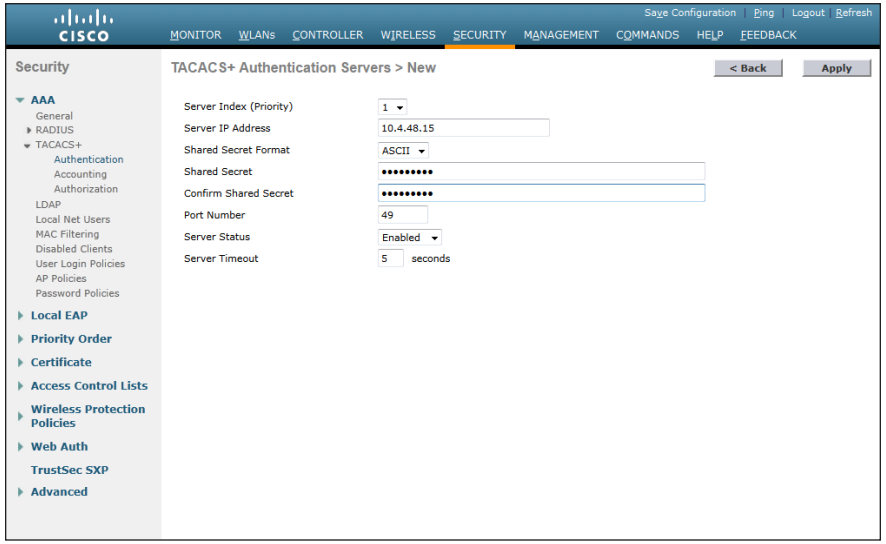
You can use this procedure to deploy centralized management authentication by configuring the Authentication, Authorization and Accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 12.

As networks scale in the number of devices to maintain, the operational burden to maintain local management accounts on every device also scales. A centralized Authentication, Authorization and Accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

Step 1: In **Security > AAA > TACACS+ > Authentication**, click **New**.

Step 2: Enter the **Server IP Address**. (Example: 10.4.48.15)

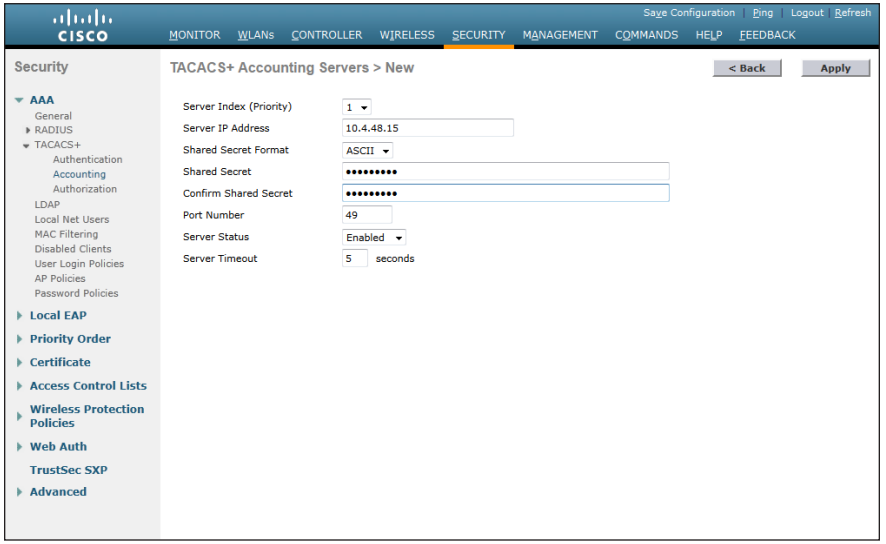
Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



Step 4: In **Security** > **AAA** > **TACACS+** > **Accounting**, click **New**.

Step 5: Enter the **Server IP Address**. (Example: 10.4.48.15)

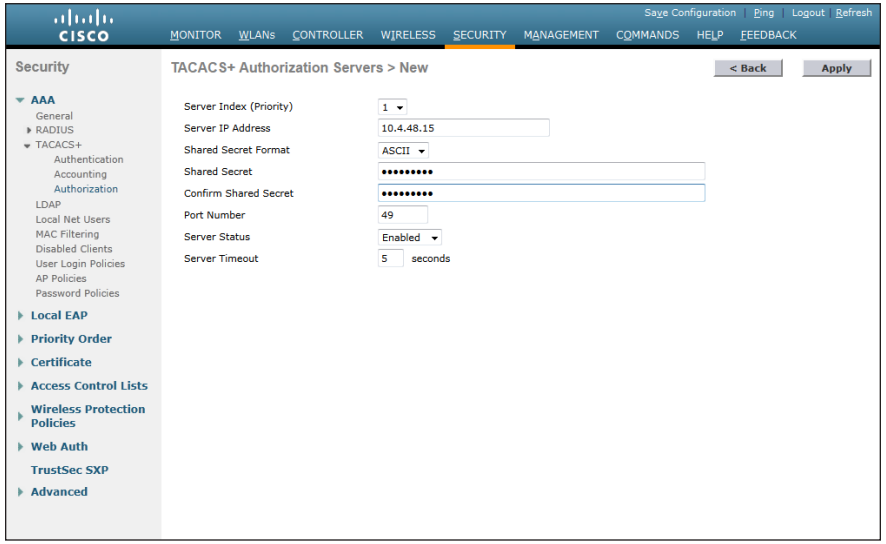
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



Step 7: In **Security** > **AAA** > **TACACS+** > **Authorization**, click **New**.

Step 8: Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 9: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

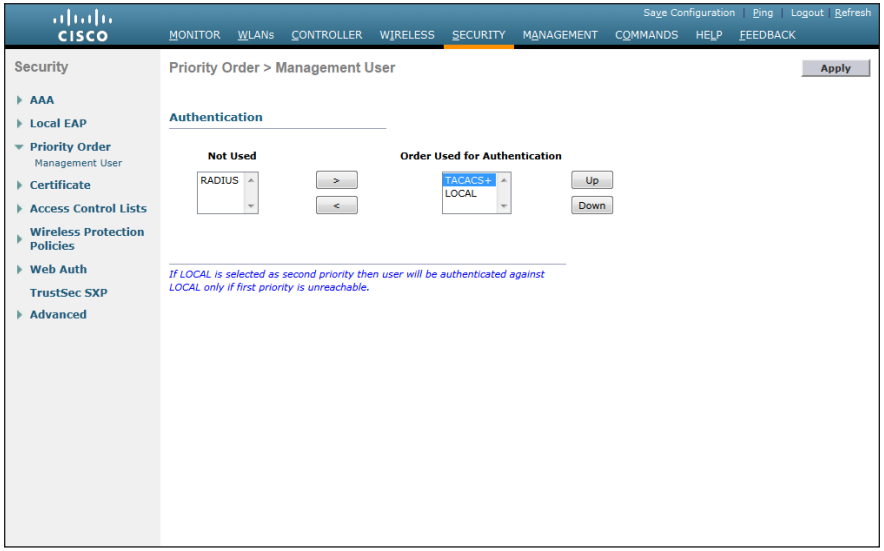


Step 10: Navigate to **Security > Priority Order > Management User.**

Step 11: Using the arrow buttons, move TACACS+ from the **Not Used** list to the **Used for Authentication** list.

Step 12: Using the **Up** and **Down** buttons, move TACACS+ to be the first in the **Order Used for Authentication** list.

Step 13: Use the arrow buttons to move RADIUS to the **Not Used** list, and then click **Apply**.



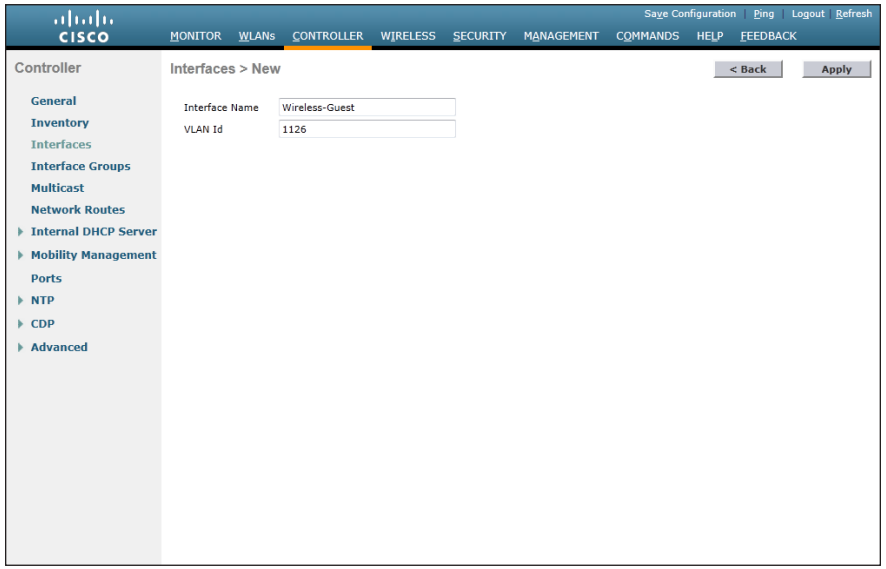
Procedure 12 Create the guest wireless LAN interface

The guest wireless interface is connected to the DMZ of the Cisco ASA 5540 security appliance. This allows guest wireless traffic only to and from the Internet. All traffic, regardless of the controller that the guest initially connects to, is tunneled to the guest WLC and leaves the controller on this interface. To easily identify the guest wireless devices on the network, use an IP address range for these clients that is not part of your organization's regular network. This procedure adds an interface that allows devices on the guest wireless network to communicate with the Internet.

Step 1: In **Controller>Interfaces,** click **New**

Step 2: Enter the **Interface Name**. (Example: Wireless-Guest)

Step 3: Enter the **VLAN identifier**, and then click **Apply**. (Example: 1128)

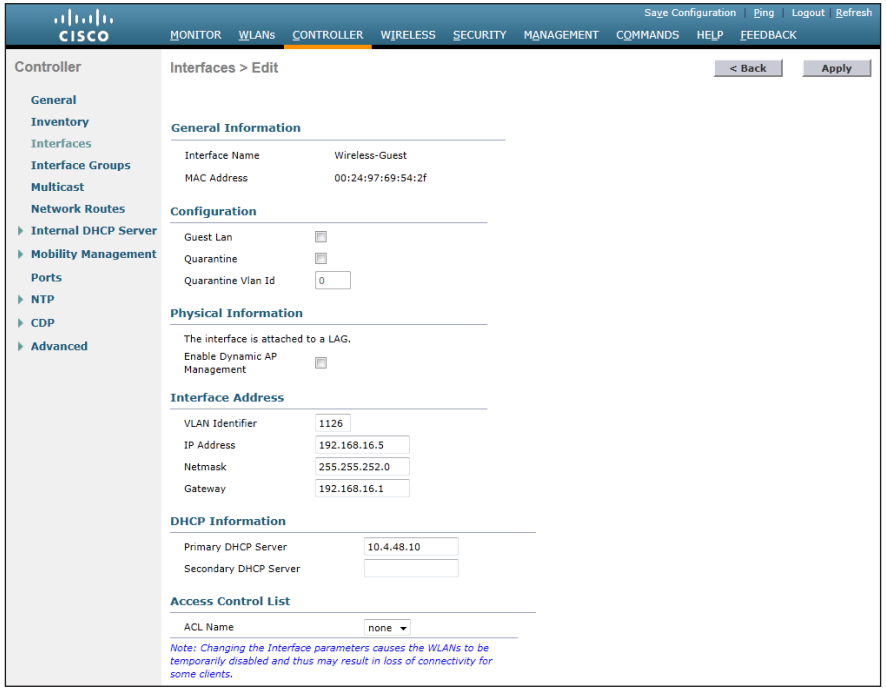


Step 4: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 192.168.28.5)

Step 5: Enter the **Netmask**. (Example: 255.255.252.0)

Step 6: In the **Gateway** box, enter the IP address of the firewall's DMZ interface defined in Procedure 2. (Example: 192.168.28.1)

Step 7: In the **Primary DHCP Server**, enter the IP address of your organization's DHCP server, and then click **Apply**. (Example: 10.4.48.10)



Tech Tip

To prevent DHCP from assigning addresses to wireless clients that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Procedure 13 Configure the guest wireless LAN

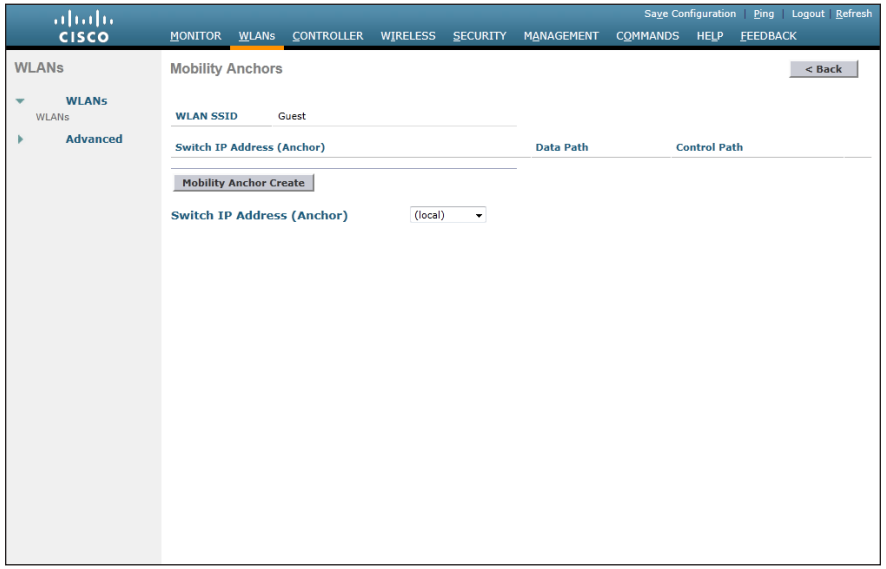
Step 1: Navigate to **WLANs**.

Step 2: Hover over the blue drop-down list next to your guest WLAN.

Step 3: Click **Mobility Anchors**.

Step 4: In the Switch IP Address (Anchor) list, choose **(local).**

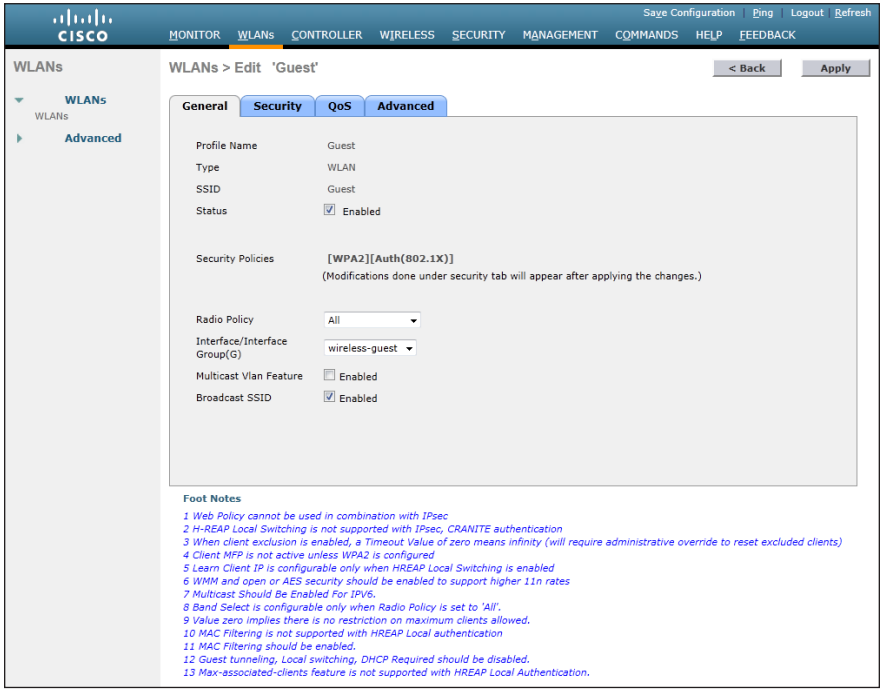
Step 5: Click **Mobility Anchor Create**, and then click **OK**.



Step 6: Click **< Back**.

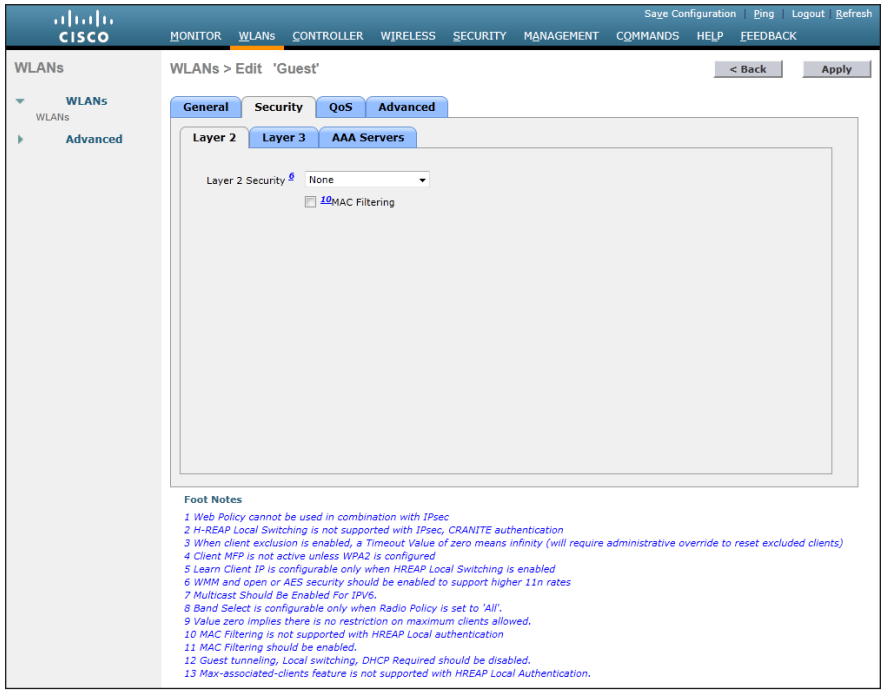
Step 7: Click the **WLAN ID** of the SSID created in Procedure 7. (Example: Guest)

Step 8: On the General tab, in the Interface list, choose the interface created in Procedure 12. (Example: Wireless-Guest)

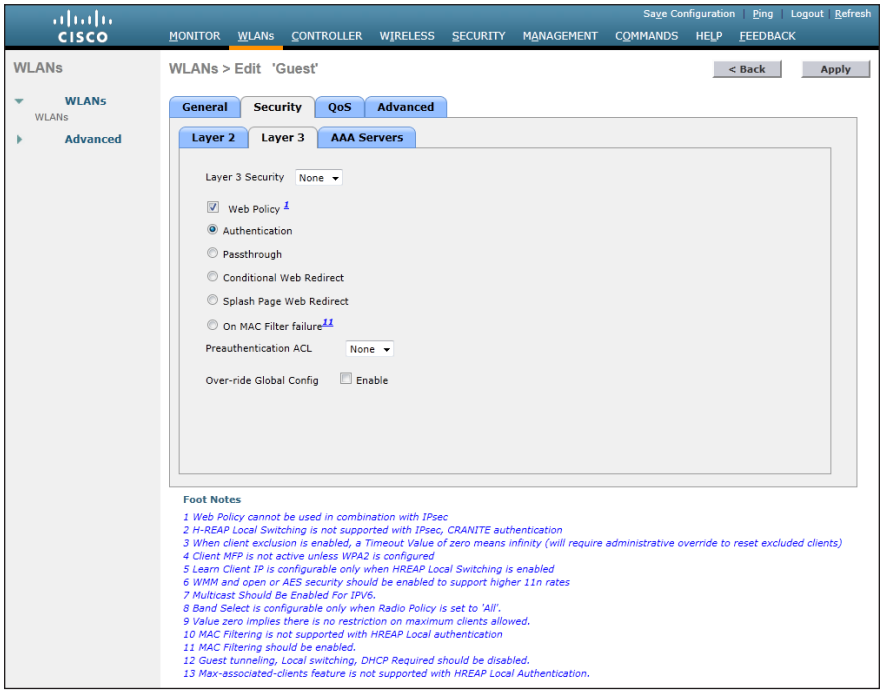


Step 9: Click the **Security** tab.

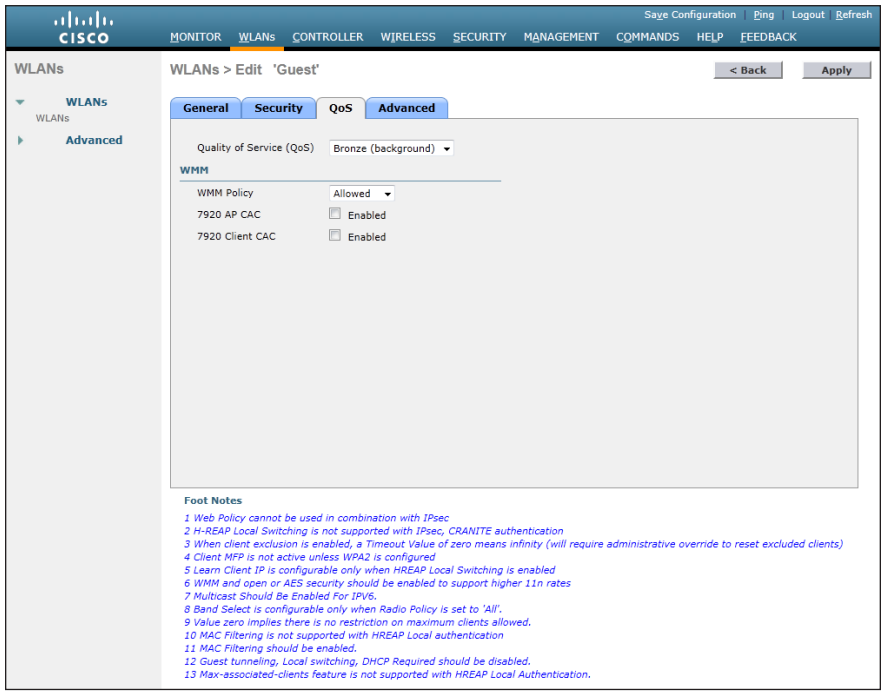
Step 10: On the Layer 2 tab, in the Layer 2 Security list, choose **None**.



Step 11: On the Layer 3 tab, select **Web Policy**, and then click **OK**.

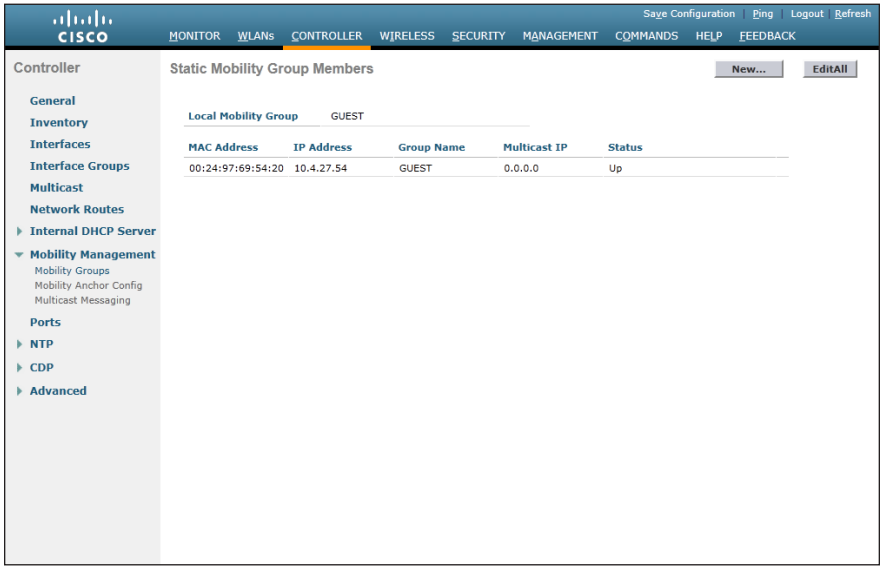


Step 12: On the QoS tab, in the Quality of Service (QoS) list, choose **Bronze (Background)**, and then click **Apply**.



Procedure 14 Configure mobility groups

Step 1: On the guest controller, navigate to **Controller > Mobility Management > Mobility Groups**. The MAC address, IP address, and mobility group name for the local controller is shown.

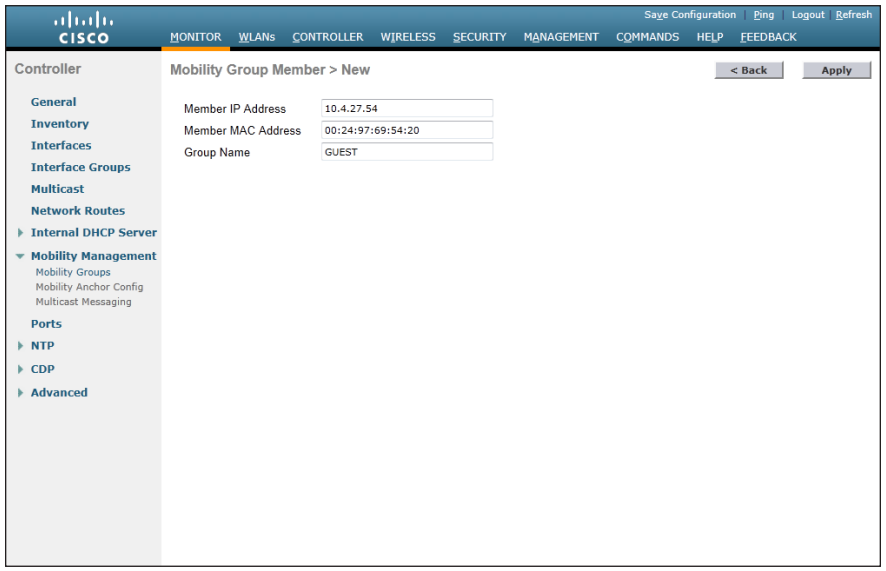


Step 2: On every other controller in your organization, navigate to **Controller > Mobility Management > Mobility Groups**, and then click **New**.

Step 3: In the **Member IP Address** box, enter the IP address of the guest controller. (Example: 192.168.19.54)

Step 4: In the **Member MAC Address** box, enter the MAC address of the guest controller.

Step 5: In the **Group Name** box, enter the mobility group name configured on the guest controller, and then click **Apply**. (Example: GUEST)

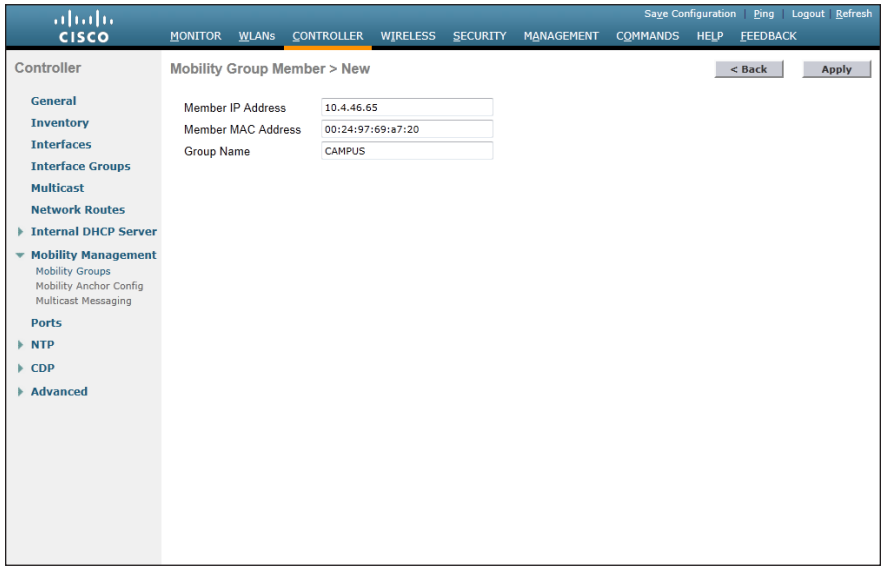


Step 6: On the guest controller, navigate to **Controller** > **Mobility Management** > **Mobility Groups**, and then click **New**.

Step 7: In the **Member IP Address** box, enter the IP address of a campus or remote-site controller. (Example: 10.4.46.65)

Step 8: In the **Member MAC Address** box, enter the MAC address of the campus or remote-site controller.

Step 9: In the **Group Name** box, enter the mobility group name configured on the campus or remote-site controller, and then click **Apply**. (Example: CAMPUS)



Step 10: On each controller, click **Save Configuration**, and then click **OK**.

Step 11: Repeat Step 6 through Step 10 on every controller in your organization.

Step 12: Navigate to **Controller** > **Mobility Management** > **Mobility Groups**, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as **Up**.

Procedure 15 Create the lobby admin user account

Typically, the lobby administrator is the first person to interact with your corporate guests. The lobby administrator can create individual guest user accounts and passwords that last from one to several days, depending upon the length of stay for each guest.

You have two options to configure the lobby admin user account.

If you have not deployed ACS and TACACS+ for management access control to the controller, perform the steps in Option 1.

If you have deployed ACS and TACACS+ for management access control to the controller, perform the steps in Option 2.

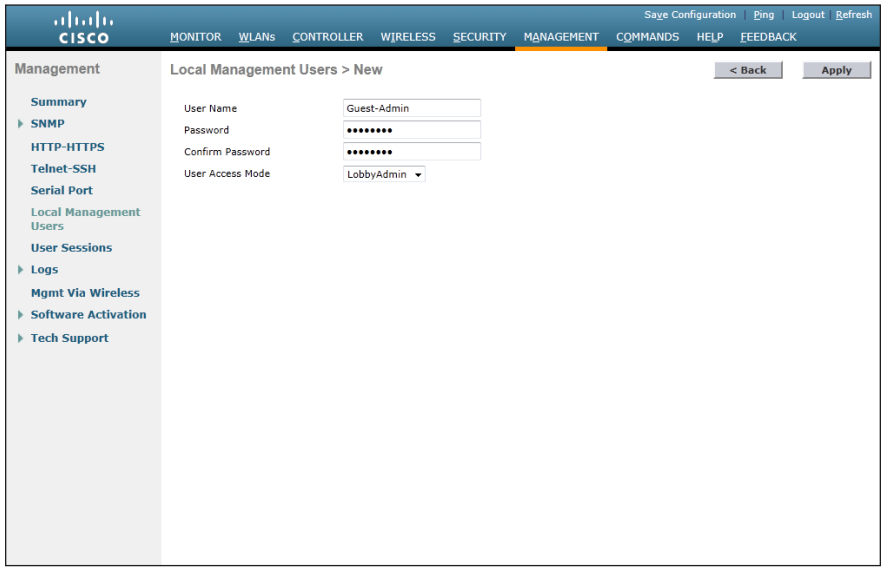
Option 1. Local lobby admin user account

Step 1: In **Management > Local Management Users**, click **New**.

Step 2: Enter the username. (Example: Guest-Admin)

Step 3: Enter and confirm the password. (Example: C1sco123)

Step 4: In the User Access Mode list, choose **LobbyAdmin**, and then click **Apply**.



Option 2. Centralized lobby admin user account

Create groups in the Cisco Secure ACS internal identity store for network device administrators and helpdesk users. Users in the network device administrator group have enable-level EXEC access to the network devices when they log in, while helpdesk users must type in the enable password on the device in order to get enable-level access.

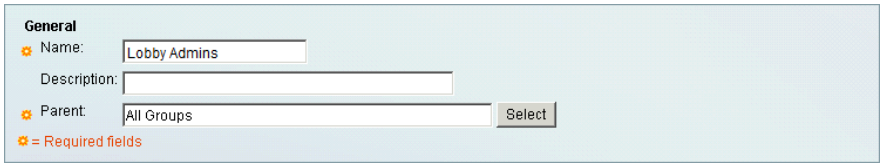
Step 1: Log in to Cisco Secure ACS via the GUI (https://acs.cisco.local).

Step 2: Navigate to **Users and Identity Stores > Identity Groups**.

Step 3: Click **Create**.

Step 4: In the Name box, enter **Lobby Admins,** and then enter a description for the group.

Step 5: Click **Submit**.



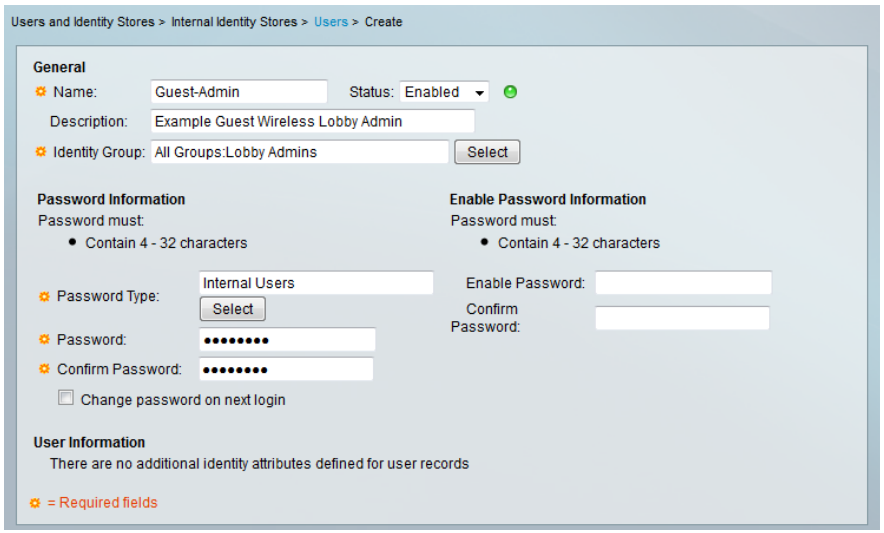
Next, you must create the lobby admin account.

Step 6: Navigate to **Users and Identity Stores > Internal Identity Stores > Users**.

Step 7: Click **Create**.

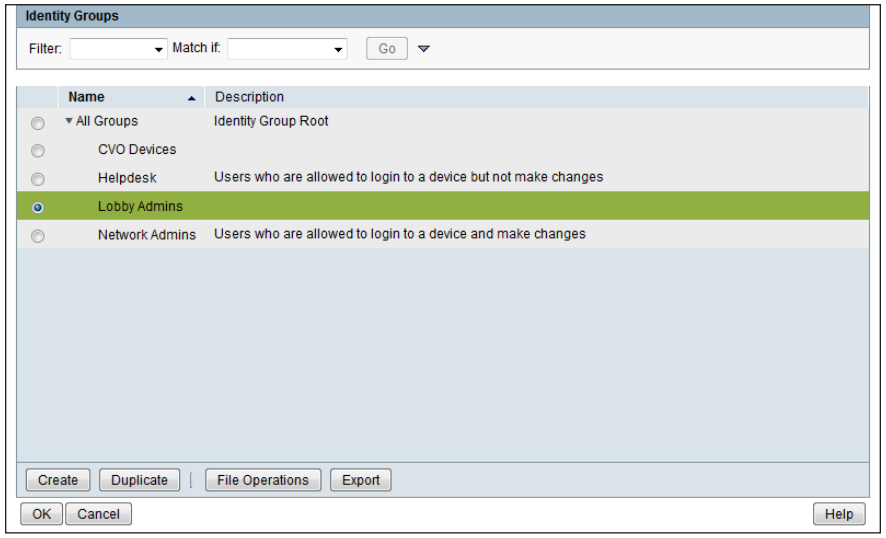
Step 8: Enter the name. (Example: Guest-Admin)

Step 9: Enter and confirm the password. (Example: C1sco123)



Step 10: To the right of Identity Group, click **Select**.

Step 11: Select the **Lobby Admins** identity group.



Step 12: Click **OK**, and then click **Submit**.

Next, you must create a shell profile for the WLCs that contains a custom attribute that assigns the user lobby admin rights when the user logs in to the WLC.

Step 13: In **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, click **Create**.

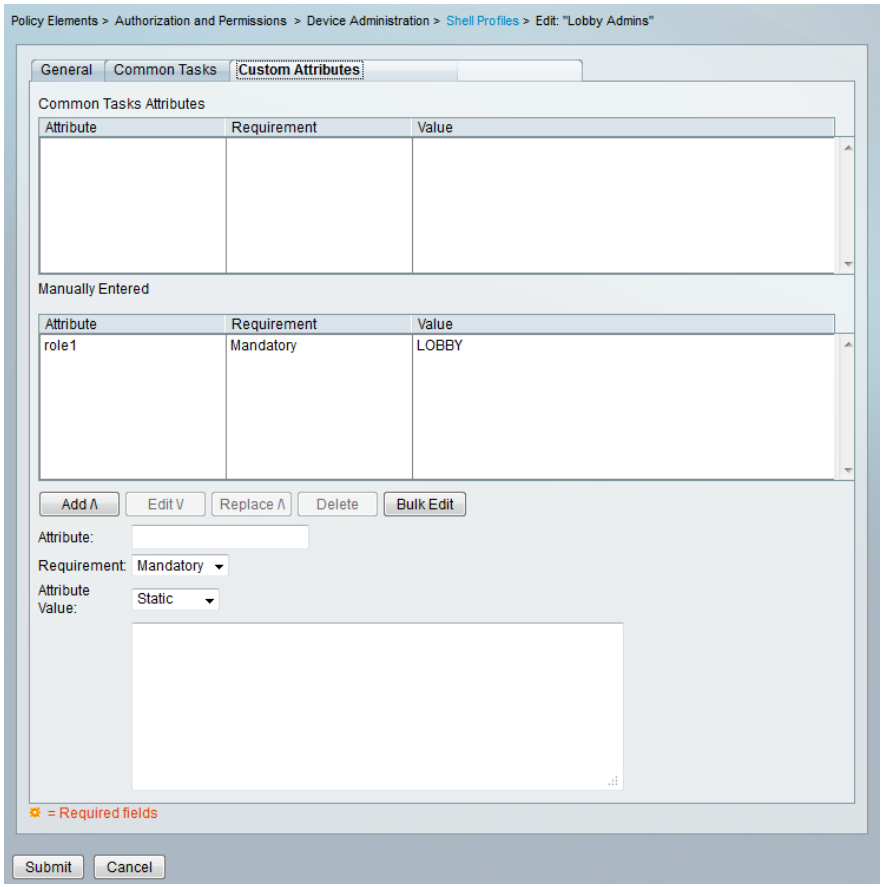
Step 14: Under the General tab, In the **Name** box, enter a name for the wireless shell profile. (Example: Lobby Admins)

Step 15: On the Custom Attributes tab, in the **Attribute** box, enter **role1**.

Step 16: In the Requirement list, choose **Mandatory**.

Step 17: In the **Value** box, enter **LOBBY**, and then click **Add**.

Step 18: Click **Submit**.



Next, create a WLC authorization rule.

Step 19: In **Access Policies > Default Device Admin >Authorization**, click **Create**.

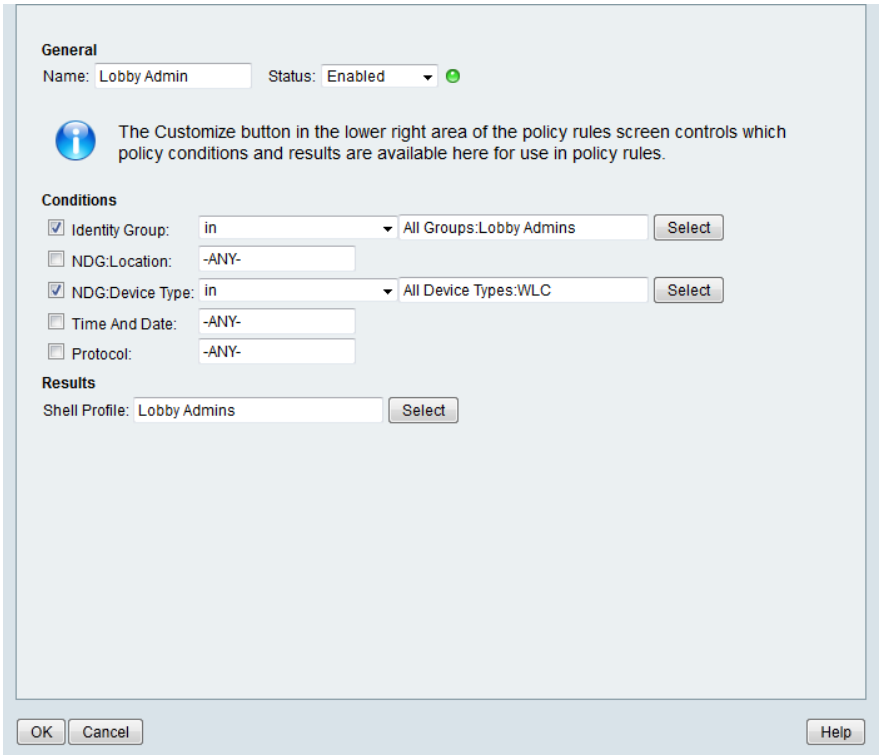
Step 20: In the **Name** box, enter a name for the WLC authorization rule. (Example: Lobby Admin)

Step 21: Under Conditions, select **Identity Group** condition, and in the box, select **Lobby Admins**.

Step 22: Select **NDG:Device Type** , and in the box, select **All Device Types:WLC.**

Step 23: In the **Shell Profile** box, select **Lobby Admins**, and then click **OK**.

Step 24: Click **Save Changes**.

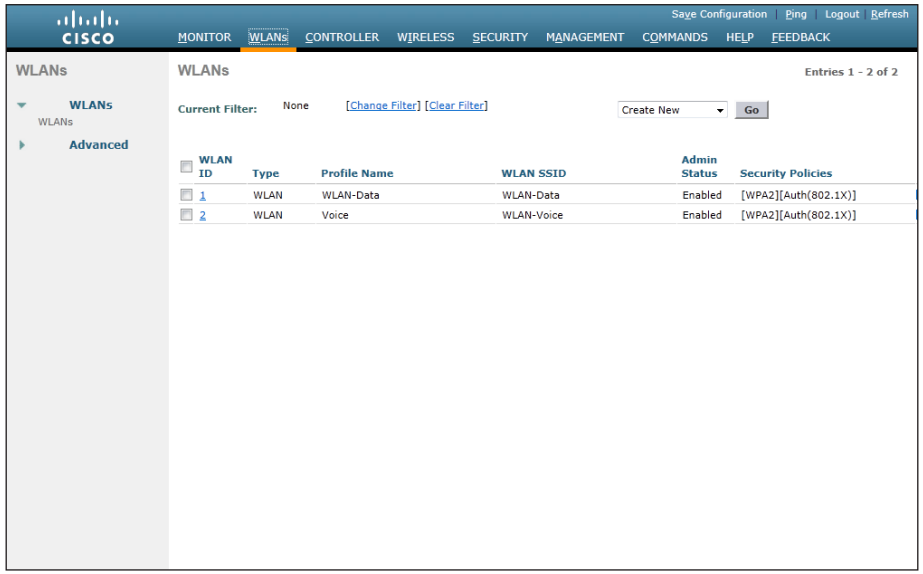


Procedure 16 Configure the internal WLCs for a guest

When a client connects to the guest SSID, the client must be anchored to the controller in the DMZ. The guest clients' traffic is tunneled in an IP-IP tunnel from the controller to which the access point is connected to the guest controller, where the access point is given an IP for the DMZ. The clients' traffic is then redirected to the web authentication page located on the guest controller. The client will not be authorized to connect with any IP protocol until it presents credentials to this authentication page.

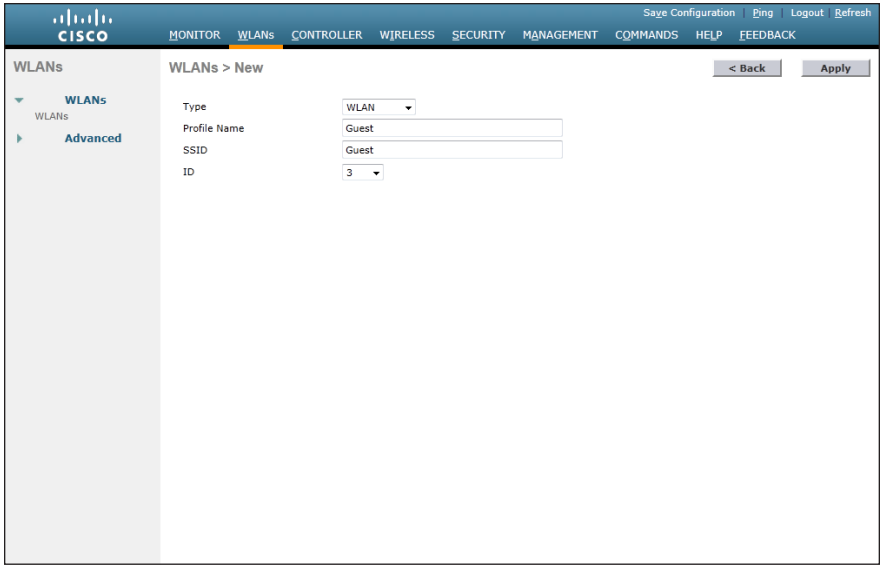
Step 1: Navigate to **WLANs**.

Step 2: In the drop-down list, choose **Create New**, and then click **Go**.



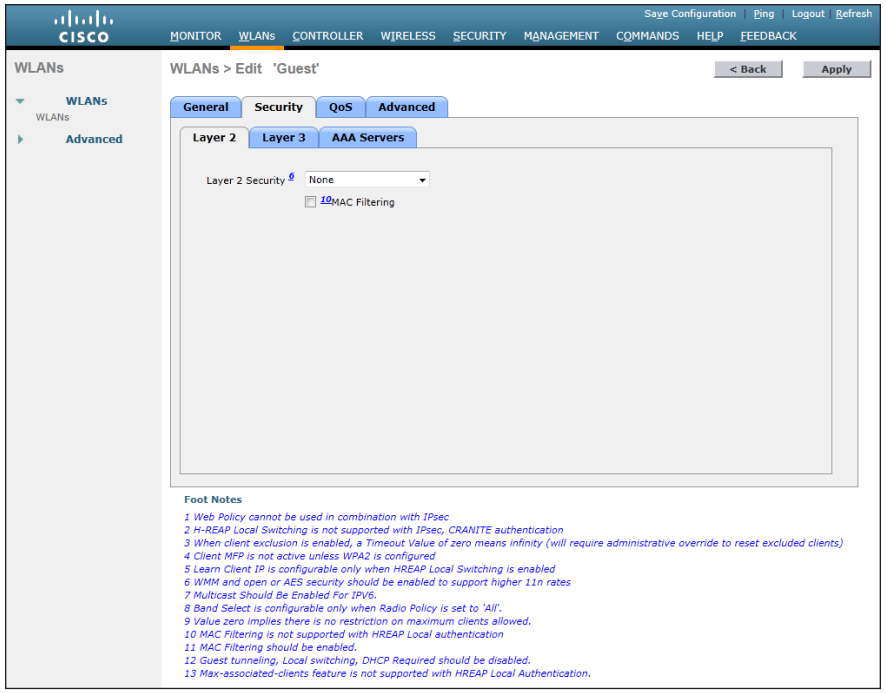
Step 3: Enter the **Profile Name**. (Example: Guest)

Step 4: In the **SSID** box, enter the guest WLAN name, and then click **Apply**. (Example: Guest)

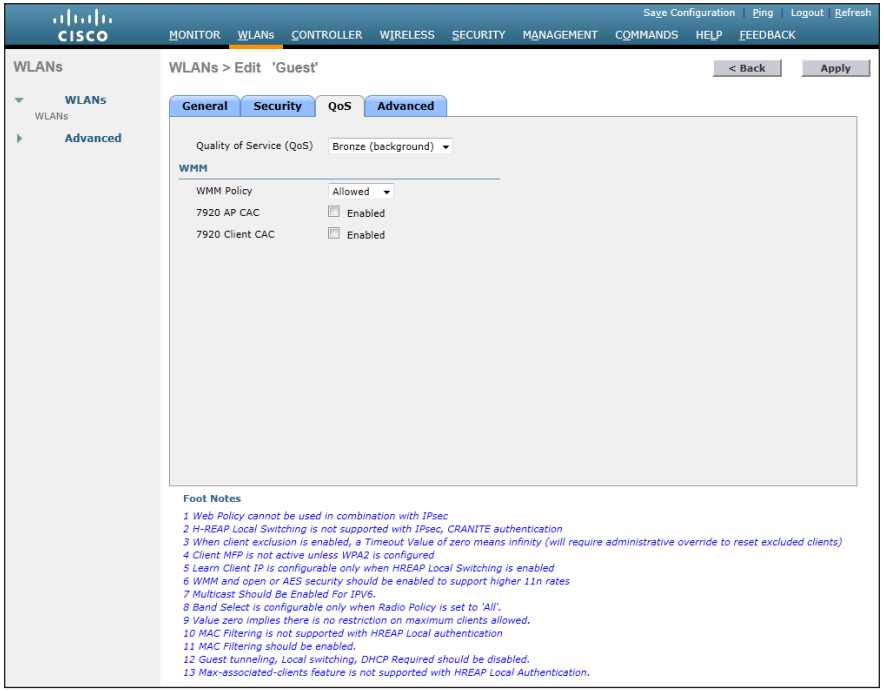


Step 5: Click the **Security** tab.

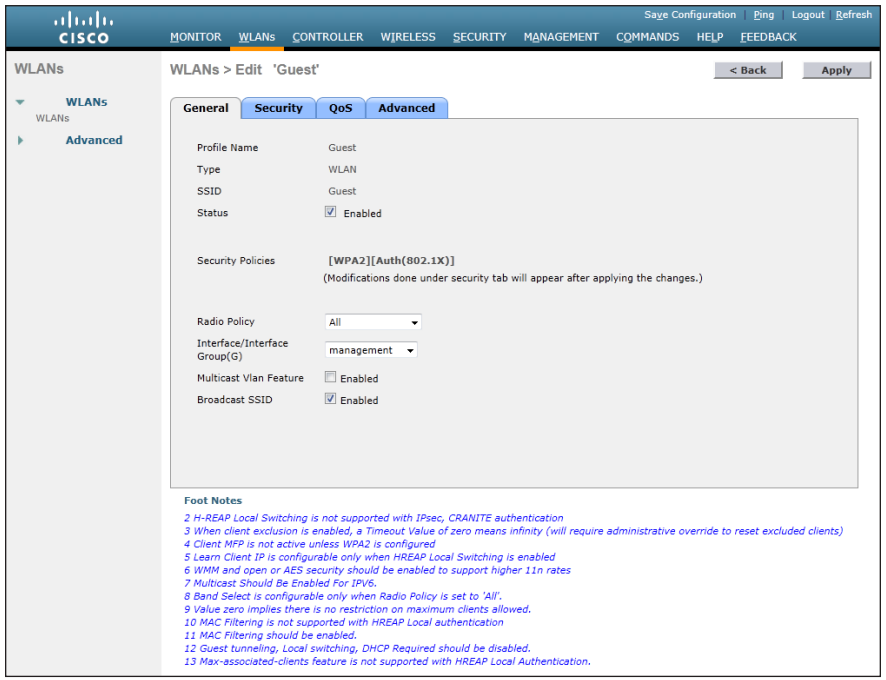
Step 6: On the Layer 2 tab in the Layer 2 Security list, choose **None**.



Step 7: On the QoS tab, in the Quality of Service (QoS) list, choose **Bronze (Background)**, and then click **Apply**.



Step 8: On the General tab, to the right of Status, select **Enabled**, and then click **Apply**.



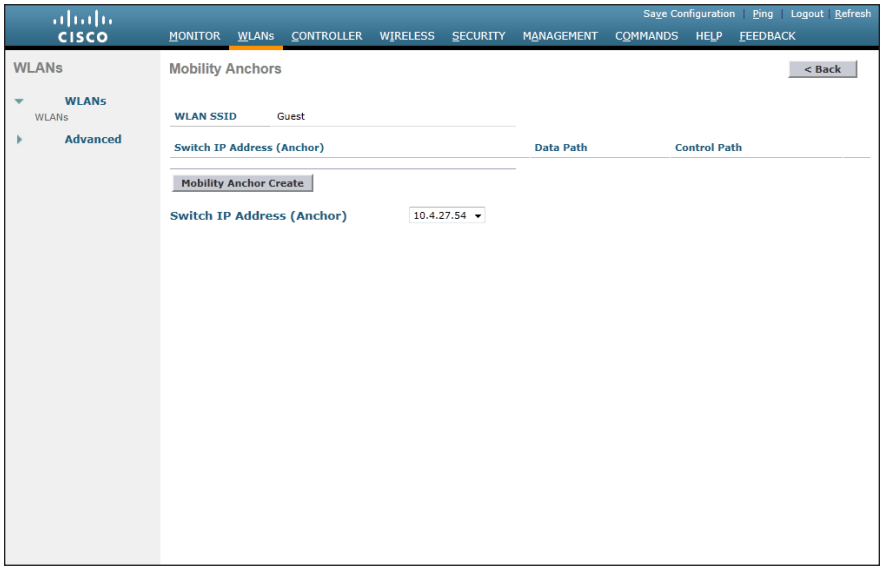
Step 9: Click **< Back**.

Step 10: Hover over the blue drop-down list next to your guest WLAN.

Step 11: Click **Mobility Anchors**.

Step 12: In the Switch IP Address (Anchor) list, choose the IP address of the guest controller. (Example: 192.168.19.54)

Step 13: Click **Mobility Anchor Create**, and then click **OK**.



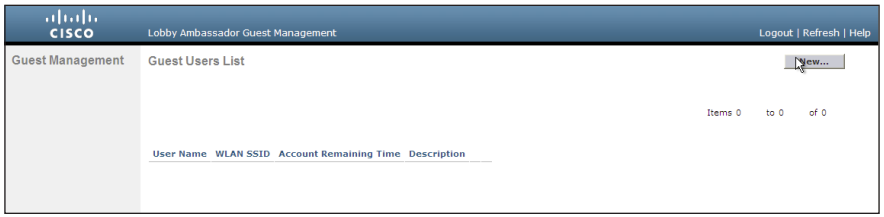
Step 14: Repeat Step 1 through Step 13 for every internal controller in your organization.

Procedure 17 Create guest accounts

Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

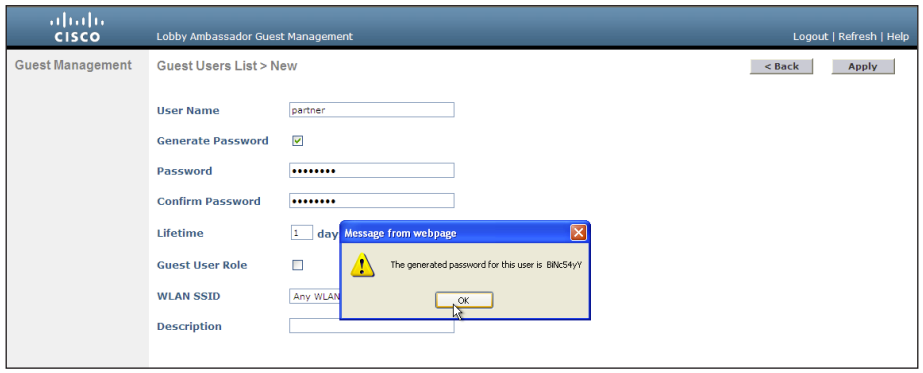
Step 1: Using a web browser, open the WLC's web interface (for example, https://guest-1.cisco.local/), and then log in using your LobbyAdmin account with the username **Guest-Admin** and password **c1sco123**.

Step 2: From the Lobby Ambassador Guest Management page, click **New**.



Step 3: Create a new username and password, or allow the system to create a password automatically by selecting **Generate Password**.

Step 4: Click Apply to create the new username



With a wireless client, you can now test connectivity to the Guest WLAN. Without any security enabled, you should receive an IP address, and—after opening a web browser— be redirected to a web page to enter a username and password for Internet access, which will be available to a guest user for 24 hours.

Notes

Appendix A: Product List

Wireless LAN Controllers

Functional Area	Product Description	Part Numbers	Software
Remote Site Controller	Cisco 7500 Series Wireless Controller for up to 3000 Cisco access points	AIR-CT7510-3K-K9	7.2.110.0
	Cisco 7500 Series Wireless Controller for up to 2000 Cisco access points	AIR-CT7510-2K-K9	
	Cisco 7500 Series Wireless Controller for up to 1000 Cisco access points	AIR-CT7510-1K-K9	
	Cisco 7500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT7510-500-K9	
	Cisco 7500 Series Wireless Controller for up to 300 Cisco access points	AIR-CT7510-300-K9	
On Site, Remote Site, or Guest Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.2.110.0
	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
On Site Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.2.110.0
	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

Wireless LAN Access Points

Functional Area	Product Description	Part Numbers	Software
CleanAir AP with 4x4 MIMO	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	7.2.110.0
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP3602E-x-K9	
CleanAir AP with 3x4 MIMO	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP2602I-x-K9	7.2.110.0
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP2602E-x-K9	
Business Ready AP	Cisco 1040 Series Access Point Dual Band 802.11a/g/n with Internal Antennas	AIR-LAP1042N-x-K9	7.2.110.0

Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.3 VMware Software and Base License	CSACS-5.3-VM-K9	5.3

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.1(3)N1(1a)
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(1)SE2 LAN Base
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1 IP services
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) Enterprise Services
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(1)SE2 IP Services
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
Modular WAN Remote-site Router	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
Modular WAN Remote-site Router	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	15.1(4)M4 securityk9, datak9
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.1(4)M4 securityk9, datak9

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We added VLAN names to match the LAN guide.
- We removed the spanning-tree root primary macro because the LAN guide has been updated to include this for all VLANs.
- We removed references to earlier procedures in the remote-site process because the SSID could be pre-existing (shared WLC) based on the new options.
- H-REAP has been rebranded Cisco FlexConnect.

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000355-1 8/12